



Federal Office
for Information Security

IT-Grundschutz Compendium

Final Draft, 1 February 2019



ISMS.1: Security Management

Description

Introduction

The planning, management and monitoring role that is essential to setting up and continuously implementing a thoroughly thought through and effective process for ensuring information security is referred to as information security management, or 'IS management' for short. A properly functioning security management process must be embedded into the existing management structures of every organisation. For this reason, it is practically impossible to specify an organisational structure for security management that is directly applicable to every organisation. Instead, it is often necessary to adapt it to the specific conditions in the organisation.

Objective

The objective of this module is to illustrate how a functioning information security management process can be established and developed further during live operation. To accomplish this, the module describes the most useful steps of a systematic security process and provides instructions for creating a comprehensive security concept.

Not in Scope

The module is based on BSI Standard 200-1 *Information Security Management Systems (ISMS)* and BSI Standard 200-2 *IT-Grundschutz Methodology* and summarises the most important aspects of security management found in these standards.

Threat Landscape

For module ISMS.1 *Security Management*, the following specific threats and vulnerabilities are of particular importance:

Lack of Personal Responsibility in the Security Process

If the roles in the security process in an organisation are not clearly defined, it is likely that many employees will deny their responsibility for information security by pointing out that the next level in the organisational hierarchy is responsible. As a result, the security safeguards are not implemented because their implementation is almost always considered at first to be an additional load on top of one's routine work.

Lack of Support from Top Management

Chief information security officers are not usually members of public authorities or top management. If the persons in charge of security do not receive unconditional support from top management, it may be difficult to effectively require the necessary safeguards to be implemented by the people directly above them in the organisational hierarchy. In such cases, it is impossible to fully implement the security process.

Inadequate Strategic and Conceptual Specifications

While many organisations create a security concept, only a few insiders are familiar with its contents in many cases. As a result, the specifications are knowingly or unknowingly not followed in locations where organisational time and effort would be required. When the security concept contains strategic security objectives, these objectives are often simply considered to be a collection of declarations of intent, and adequate resources are not provided for their implementation as a result. In many cases, it is incorrectly assumed that security is achieved automatically in an automated environment. Damage events in the organisation or in similarly structured organisations will occasionally trigger more or less fervent activity in which only some sub-aspects at the most are actually improved upon.

Inadequate or Misdirected Investments

If the top management of an organisation is not adequately informed of the security status of business processes, IT systems, applications and existing shortcomings, an insufficient amount of resources will be provided for the security process, or the resources will not be used properly. In the latter case, this may result in a situation where one area has an excessive level of security, while other areas have serious security shortcomings. It is commonly observed that expensive technical security solutions are used incorrectly and are therefore rendered ineffective, or even pose a security risk.

Inadequate Enforcement of Security Safeguards

In order to reach a consistent and adequate level of security, it is necessary for various areas of responsibility in an organisation to cooperate. A lack of strategic guidance statements and unclear objectives can lead to different interpretations of the importance of information security, among other things. Consequently, it is possible that the areas of responsibility required to cooperate will not assume the task of providing information security due to a supposed lack of necessity or poor prioritisation, and thereby make it impossible to enforce the implementation of the security safeguards.

Failure to Update the Security Process

New business processes, applications and IT systems, as well as new basic threats, constantly affect the status of information security within an organisation. If there is no effective audit concept that also increases awareness of the new basic threats, the security level will fall and the actual level of security will gradually become a dangerous illusion of security.

Violation of Statutory Regulations and Contractual Agreements

If the information, business processes and IT systems of an institution are inadequately protected (for example, as a result of inadequate security management), this can result in violations of regulations relating to information processing or of existing contracts with business partners. The laws that apply depend on the type of organisation and its business processes and services.

Depending on the locations of the organisation, various national and international regulations may need to be followed. If an organisation has insufficient knowledge of international legal requirements (e.g. those regarding data protection, the duty to supply information, insolvency law, liability or access to information for third parties), this increases the risk of corresponding violations. There is a threat of legal consequences.

In many industries, it is common for users to require their suppliers and service providers to comply with certain quality and safety standards. In this context, requirements regarding information security are also being specified to an increasing extent. If a contract partner fails to meet contractually regulated security requirements, this can result in contractual penalties, but also contract terminations or even the loss of business relationships.

Business Process Disruptions Due to Security Incidents

Security incidents can be triggered by a singular event or a chain of unfortunate circumstances and can have a negative impact on the confidentiality, integrity or availability of information and IT systems. This will then quickly have an adverse effect on essential specialised tasks and business processes in the organisation affected. Even if most of the security incidents do not become public, the incidents that do become public may still have a negative impact on the organisation's relationships with business partners and customers. It is not even true that the most serious and extensive security incidents are triggered by the most serious security vulnerabilities. In many cases, a chain reaction of minor factors will lead to the most extensive damage.

Uneconomic Use of Resources Due to Inadequate Security Management

Inadequate security management can lead to the wrong priorities being set and investments not being made in areas that bring the greatest benefits to the organisation. This may lead to the following errors:

- An organisation may invest in expensive security solutions without providing for the basic organisational regulations required. When not clearly defined, competencies and responsibilities can still lead to serious security incidents in spite of a high investment.
- An organisation may invest in information security in areas which are particularly aware of information security. Other areas that are important to carrying out the business processes and reaching the business objectives may be ignored due to a lack of resources or a lack of interest on the part of the persons in charge.
- Investments may only be made in individual sub-areas. However, there may still be significant vulnerabilities in the overall system.
- The overall level of protection may drop when emphasis is only placed on increasing the level of protection for individual key security objectives.
- The inconsistent and uncoordinated use of security products may result in high use of financial and personnel resources.

Requirements

The specific requirements of module ISMS.1 *Security Management* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for fulfilling the re-

quirements. Deviations from this are mentioned separately in the respective requirements. The CISO must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Top Management, Supervisor

Basic Requirements

For module ISMS.1 *Security Management*, the following requirements **MUST** be implemented as a matter of priority:

ISMS.1.A1 Top Management Acceptance of Overall Responsibility for Information Security [Top Management]

The top management **MUST** accept the overall responsibility for information security in the organisation in a way that can be clearly recognised by all parties involved. The organisation's top management **MUST** initiate, control and monitor the security process. The top management **MUST** set a good example regarding information security.

The top management of the public authority or company **MUST** appoint the employees responsible for information security and provide them with the necessary authority and resources. The top management **MUST** regularly obtain information on the status of information security, particularly with regard to possible risks and consequences of a lack of security safeguards.

ISMS.1.A2 Defining Security Objectives and Strategy [Top Management]

The security process **MUST** be initiated and established by the top management. For this purpose, it is necessary to specify and document adequate security objectives and a strategy for information security. Conceptual specifications **MUST** be developed and the general organisational conditions needed **MUST** be created to enable the proper and secure handling of information in all business processes of the company or public authority.

The organisation's top management **MUST** support and take responsibility for the security strategy and objectives. The security objectives and security strategy **MUST** be examined regularly to determine if they are still appropriate and up to date and can be implemented effectively.

ISMS.1.A3 Drawing Up an Information Security Policy [Top Management]

The top management **MUST** adopt a higher-level policy for information security that describes the value of information security, the security objectives, the most important aspects of the security strategy and the organisational structure for information security. The scope of the security policy **MUST** be clearly defined. In the policy for information security, the security objectives and how they relate to the business objectives and tasks of the organisation **MUST** be explained.

The policy for information security MUST be made available to all employees and other members of the organisation. It SHOULD be updated regularly.

ISMS.1.A4 Appointment of a Chief Information Security Officer [Top Management]

The top management MUST appoint a Chief Information Security Officer who promotes information security in the organisation and controls and coordinates the security process. The Chief Information Security Officer MUST be provided with adequate resources. They MUST have the possibility to directly report to the top management if needed. The Chief Information Security Officer MUST be adequately qualified and MUST have sufficient opportunities to improve their skills.

The Chief Information Security Officer MUST be involved at an early stage in all larger projects, as well as when introducing new applications and IT systems.

ISMS.1.A5 Contract Design When Appointing an External Chief Information Security Officer [Top Management]

If the role of Chief Information Security Officer cannot be filled by an internal employee, an external Chief Information Security Officer MUST be appointed. The service contract agreed to this end MUST cover all tasks of the Chief Information Security Officer and the associated rights and obligations. The contract MUST include an appropriate non-disclosure agreement. The external Chief Information Security Officer MUST have the required qualifications. The contract MUST ensure the controlled termination of the contract relationship, including the handover of tasks to the customer.

ISMS.1.A6 Establishment of a Suitable Organisational Structure for Information Security [Top Management]

A suitable overall organisational structure for information security MUST be in place. To this end, roles MUST be defined to perform the various tasks required to achieve the security objectives. In addition, qualified people MUST be appointed who have sufficient resources in order to carry out these roles. The tasks, responsibilities and competencies in security management MUST be defined and assigned in a transparent manner. Effective substitution arrangements MUST be in place for all important functions of the IS organisation.

The communication channels MUST be planned, described, set up and announced. For all tasks and roles, it MUST be specified who will inform whom, who must be informed of which actions and the required scope of the information provided.

It MUST be checked at regular intervals whether the organisational structure for information security is still adequate or needs to be adapted to new framework conditions.

ISMS.1.A7 Definition of Security Safeguards

As part of the security process, detailed and adequate security safeguards MUST be defined for all aspects of information processing. All security safeguards SHOULD be documented systematically in security concepts and updated at regular intervals.

ISMS.1.A8 Integration of Employees into the Security Process [Supervisor]

All employees MUST be integrated into the security process, meaning they must be informed of the backgrounds and threats and know and implement security safeguards relating to their workplaces. They MUST be enabled to take an active role in security, including by incorporat-

ing this subject into their business processes. The employees SHOULD therefore be involved in the early stages of planning security safeguards or developing organisational rules.

When introducing security policies and security tools, the employees MUST be adequately informed about how these should be used.

ISMS.1.A9 Integrating Information Security into Organisation-Wide Procedures and Processes [Top Management]

Information security MUST be integrated into all business processes. In so doing, it MUST be ensured that all necessary security aspects are not only taken into account in new processes and projects, but also in ongoing activities. Moreover, information security SHOULD be coordinated with other areas in the organisation that deal with security and risk management.

The Chief Information Security Officer MUST be adequately involved in making security-relevant decisions.

Standard Requirements

For module ISMS.1 *Security Management*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

ISMS.1.A10 Drawing Up a Security Concept

For the specified scope (of the information domain), an adequate security concept SHOULD be drawn up as the central document in the security process. The security concept may also consist of several sub-concepts which are drawn up successively to establish the required level of security in selected areas first.

In the security concept, specific security safeguards appropriate for the information domain under consideration MUST be derived from the security objectives of the organisation, the protection needs identified and the risk evaluation conducted. The security process and the security concept MUST take the individually applicable regulations and provisions into account.

The safeguards provided in the security concept MUST be implemented promptly in practice. Their implementation MUST be planned and monitored. It SHOULD be checked regularly whether the selected safeguards are appropriate, adequate, realisable and efficient in order to achieve the security objectives and requirements.

Every employee SHOULD have at least been informed of the parts of the security concept that apply to them.

ISMS.1.A11 Continuity of Information Security

The security process, the security concepts, the information security policy and the organisational structure for information security SHOULD be reviewed in terms of their appropriateness and effectiveness and updated at regular intervals. Completeness and update checks of the security concept SHOULD be performed regularly in this regard. Security audits SHOULD also be performed regularly. In this regard, there SHOULD be rules specifying which areas and security safeguards will have to be checked when and by whom. The level of security SHOULD be reviewed regularly (at least once a year) and whenever there is a reason to do so.

The reviews SHOULD be performed by qualified and independent persons. The results of the reviews SHOULD be documented in a transparent manner. On this basis, shortcomings SHOULD be remedied and corrective measures taken.

ISMS.1.A12 Management Reports on Information Security [Top Management]

Top management SHOULD regularly be informed about the status of information security – especially in terms of the current threat landscape and the effectiveness and efficiency of the security process – in order to control the subsequent security process. The management reports SHOULD contain the most important information relevant to the security process, particularly with regard to information about problems, successes and potential improvements. They SHOULD include clearly prioritised suggestions for safeguards, along with a realistic estimate of the amount of time and expense required to implement them.

The management decisions relating to required actions, the handling of residual risks and changes to security-relevant processes SHOULD be documented. The management reports and management decisions SHOULD be archived in an audit-compliant manner.

ISMS.1.A13 Documentation of the Security Process

The sequence of events in the security processes, important decisions and the work results of the individual phases (such as the security concept, policies, or findings from examinations of security incidents) SHOULD be documented adequately.

A procedure SHOULD be defined for the creation and archiving of documentation within the framework of the security process. Rules SHOULD be in place to ensure that documentation is up-to-date and kept confidential. The respective current version of existing documents SHOULD be available on short notice. Furthermore, all previous versions SHOULD be archived centrally.

ISMS.1.A14 Raising Awareness of Information Security

The security risk awareness of all organisation employees and other relevant persons (such as external employees or project members) SHOULD be raised systematically and in a suitable manner for the respective target group. These individuals SHOULD also be trained in aspects of information security (see ORP.3 *Awareness and Training*).

ISMS.1.A15 Cost-Effective Use of Resources for Information Security

Information security requires sufficient financial and personnel resources, as well as suitable equipment. The needs SHOULD be communicated by the CISO to the top management, which SHOULD in turn provide the required resources.

The security strategy SHOULD take economic aspects into account. When the security safeguards are defined, the resources required for their implementation SHOULD also be quantified. The resources planned for information security SHOULD be provided on time. The Chief Information Security Officer or the information security management team MUST have sufficient time to perform their security tasks. In case of workload peaks or special tasks, additional internal employees or external experts SHOULD be used.

Requirements in Case of Increased Protection Needs

Generic suggestions for module ISMS.1 *Security Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a

risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

ISMS.1.A15 Creating Target-Group-Oriented Security Policies (CIA)

All employees SHOULD know and observe the security aspects affecting their area of responsibility. In order to convey security issues in a target-group-oriented manner, there SHOULD be target-group-oriented security policies (in addition to the general policies) that map the relevant security issues as required.

ISMS.1.A17 Acquiring Insurance (A)

It SHOULD be examined whether insurance needs to be taken out against residual risks to cover any eventual damage. The existing insurance policies SHOULD be checked regularly to ensure they are still appropriate for the current situation.

Additional Information

For more information about threats and security safeguards for module ISMS.1 *Security Management*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[27002]	ISO/IEC 27002:2013: Information technology - Security techniques - Code of practice for information security controls, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[BSI1]	Information Security Management Systems (ISMS), BSI Standard 200-1, Version 1.0, October 2017, https://www.bsi.bund.de/grundschutz
[BSI2]	[BSI2] IT-Grundschutz Methodology, BSI Standard 200-2, Version 1.0, October 2017, https://bsi.bund.de/grundschutz

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module ISMS.1 *Security Management*:

G 0.18 Poor Planning or Lack of Adaptation

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

Elementary Threats Requirements	G 0.18	G 0.27	G 0.29
ISMS.1.A1	X	X	
ISMS.1.A2	X		
ISMS.1.A3	X		
ISMS.1.A4	X	X	
ISMS.1.A5	X		
ISMS.1.A6	X		
ISMS.1.A7	X		
ISMS.1.A8	X		X
ISMS.1.A9	X		
ISMS.1.A10	X		
ISMS.1.A11	X		X
ISMS.1.A12			X
ISMS.1.A13	X		
ISMS.1.A14			X
ISMS.1.A15	X		X
ISMS.1.A16	X	X	
ISMS.1.A17	X		



ORP.1: Organisation

Description

Introduction

Each company and each public authority must have an organisation that controls the interaction between its different roles and units and its business processes and resources. Most organisations have an organisational unit which is responsible for regulating and monitoring general operations and planning, organising and providing all administrative services. Various information security tasks must be implemented or supported by this unit.

Objective

This module describes requirements that are designed to enable an organisation to adequately control and maintain information security.

Not in Scope

In this module, general and comprehensive organisational requirements for establishing information security are listed. To achieve this, information flows, processes, the distribution of roles and the structural and procedural organisation must be regulated. The module Organisation thus constitutes the framework for the implementation of information security based on other modules. Special organisational requirements that are directly related to the requirements of other modules (e.g. *Server Administration*) are presented in the corresponding modules.

Threat Landscape

For module ORP.1 *Organisation*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Rules

The importance of comprehensive organisational rules and specifications in achieving information security (e.g. regarding responsibilities or the distribution of control tasks) increases with the complexity of the business processes and the scope of information processing, but also with the protection needs of the information to be processed.

A lack of rules can result in severe vulnerabilities because employees do not know how they should react if there is an incident, for example. Problems can also result from rules which are outdated, impracticable or not clearly formulated.

Ignored Rules

Merely defining rules does not ensure that they will be followed. All employees must be familiar with the applicable rules. Damage resulting from a lack of knowledge of the existing rules cannot be excused by simply saying "I didn't know I was responsible for that" or "I didn't know what to do".

Examples of damage resulting from ignored rules include:

- Confidential information being discussed within earshot of outsiders – for example, while talking during a break in a meeting or talking on a mobile telephone in a public environment
- Documents being published on a web server without checking whether or not they are actually intended and approved for publication
- An employee who is able to modify data without realising the possible critical impact of a violation of integrity due to incorrect administration of access rights

Non-Existent, Inadequate or Incompatible Resources

Failures to provide enough resources may significantly disrupt operations. Disruptions may occur if the required resources are not available in sufficient quantities are not provided quickly enough. In some cases, unsuitable or even incompatible resources are also purchased that cannot be used as a result.

Example: The storage space available on the hard disks of PCs, servers and mobile storage media is constantly increasing. Unfortunately, people often neglect to purchase IT components and storage media with enough capacity for use as regular backup media.

The proper functioning of the resources used must also be ensured. Inadequate maintenance (or none at all) may lead to significant damage.

Examples:

- The batteries of an uninterruptible power supply (UPS) system no longer have enough capacity (not enough acid content) due to a lack of maintenance. As a result, the UPS system can no longer ensure the supply of power for a sufficiently long period when there is a power failure.
- Due to a lack of maintenance, the pressure of fire extinguishers drops to a point where their fire-fighting capability is no longer guaranteed.

Unauthorised Admission to Sensitive Rooms

All rooms in which sensitive information is stored or processed further, including rooms in private homes and other external locations that are used for company purposes, must be protected against unauthorised third-party access. Unauthorised persons can cause damage deliberately through manipulation or vandalism, but also inadvertently due to human error (due to a lack of skills or the knowledge required). Even when there is apparently no immediate damage, operations can still be disrupted if it is necessary to examine how such an event was possible, whether damage occurred or whether data or devices were manipulated.

Intruders could have, for example, reset passwords, accessed the servers directly or manipulated active network components. In addition, they could have stolen or altered sensitive information stored on paper or on storage media.

Unauthorised Use of Rights

Rights such as site, system and data access authorisations are used as organisational safeguards to protect information, business processes and IT systems against unauthorised access. If these rights are granted to the wrong person or a right is exercised without authorisation, this may result in a number of threats. For example, unauthorised persons could get access to personnel data.

Threats Posed by External Individuals

In cases involving external individuals, it cannot be assumed that they will handle information and information technology according to the rules specified by the organisation they are visiting, especially because they seldom know these rules.

Visitors, cleaning staff, and external personnel can pose a hazard to internal information, business processes and systems in various ways, ranging from the improper handling of technical equipment and attempts to "play" with IT systems to the theft of documents or IT components.

Examples:

- Unaccompanied visitors could obtain access to documents, storage media or devices and damage them or gain knowledge of sensitive information without authorisation.
- Cleaning staff may accidentally unplug a cable connection, water may leak into equipment or documents may be misplaced or even taken out with the usual rubbish.

Manipulation of Information and Devices

External and internal attackers can use shortcomings in the organisation and try to manipulate devices, accessories, documents or other storage media. Manipulations can range from collecting data incorrectly or changing access rights to manipulating operating systems, storage media or IT systems. The later such attacks are detected, the greater the knowledge acquired by the perpetrator, the more far-reaching the impact on the respective process and the more effective the attacks will be.

Example: In a Swiss financial company, the application software for certain financial services was manipulated by an employee. This made it possible for him to obtain sizeable amounts of money illegally.

Destruction, Vandalism, Sabotage

Persons may try to impair business processes or manipulate or destroy devices or information for various reasons (revenge, ill will, frustration).

External attackers (such as disappointed burglars or demonstrators that get out of control) as well as internal attackers (such as frustrated or psychologically unstable employees) can destroy or damage someone else's property as perpetrators of vandalism. Whereas vandalism is usually the result of spontaneous, blind destructiveness, sabotage refers to the intentional ma-

nipulation or damaging of objects with the aim of inflicting damage on the victim. Data centres or communications links owned by public authorities or companies make particularly attractive targets of sabotage because a dramatic effect can be achieved with relatively little effort.

Theft and Loss of Information and Devices

In addition to direct material losses, the theft or loss of storage media, IT systems or data can lead to different types of damage if no adequate organisational precautions have been taken.

Requirements

The specific requirements of module ORP.1 *Organisation* are listed below. As a matter of principle, the Chief Information Security officer (CISO) is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements.

Module Owner	Head of Organisation
Further Roles	Chief Information Security Officer (CISO), IT Operation Department, Head of Production and Manufacturing, Top Management, Head of Building Services, Employee, ICS Information Security Officer, Head of IT, Building Services

Basic Requirements

For module ORP.1 *Organisation*, the following requirements **MUST** be implemented as a matter of priority:

ORP.1.A1 Specification of Responsibilities and Provisions [Top Management]

For all security-relevant tasks, both responsibilities and competences **MUST** be specified. Binding provisions regarding information security **MUST** be defined globally for the different operational aspects. Which information may be exchanged with whom and how it should be protected **MUST** also be clearly regulated. The rules **MUST** be updated at regular intervals. All employees **MUST** be informed of these provisions.

ORP.1.A2 Assignment of Responsibility for Information, Applications, and IT Components [Head of IT, Chief Information Security Officer (CISO), Top Management]

For all information, business processes, applications and IT components, it **MUST** be specified who is responsible for them and their security. In particular, all employees **MUST** be informed of what they are responsible for and how they are responsible for it.

ORP.1.A3 Supervising or Escorting External Individuals [Employee]

The employees **MUST** be required to ensure that external individuals are not left unsupervised.

ORP.1.A4 Separation of Roles Between Operative and Controlling Tasks

Within an organisation, all relevant tasks and roles **SHOULD** be defined and clearly separated from each other. The tasks and the roles and functions they require **MUST** be structured in

such a way that operative and controlling roles are assigned to different persons. The separation of roles involving conflicts **MUST** be defined and documented. Representatives **MUST** also be subject to the separation of roles.

ORP.1.A5 Granting Authorisations [Head of IT]

It **MUST** be defined which site, system and data access rights are to be granted to which persons as part of their tasks and roles. Only as many rights as are necessary to perform the corresponding tasks **MAY** be granted. There **MUST** be a controlled procedure for granting, managing and withdrawing authorisations (see also ORP.4 *Identity and Access Management*). The documentation of the authorisations **MUST** be up to date and complete.

Standard Requirements

For module ORP.1 *Organisation*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

ORP.1.A6 Clean Desk Policy [Employee]

It **SHOULD** be pointed out to all employees that neither sensitive information nor IT systems may be openly accessible at unattended workstations. Workstations **SHOULD** be checked sporadically to verify whether sensitive information is openly accessible.

ORP.1.A7 Device Management [Head of IT, Head of Production and Manufacturing, Head of Building Services]

There **SHOULD** be an overview of all devices which are used in the organisation and may have an impact on information security. In addition to IT systems and ICS components, this also includes devices related to the Internet of Things. There **SHOULD** be suitable verification and approval processes before the devices are used.

ORP.1.A8 Resource Management [Head of IT]

The resources required for performing tasks and complying with the security requirements **SHOULD** be available in insufficient quantities. There **SHOULD** be suitable verification processes before the resources are used. Resources **SHOULD** be maintained in inventory lists. In order to prevent any misuse of data, rules **SHOULD** be established relating to the deletion or destruction of resources.

ORP.1.A9 Correct Disposal of Sensitive Resources [Employee, Chief Information Security Officer (CISO)]

Resources and equipment **SHOULD** be disposed of in such a way that no conclusions can be drawn regarding their use or content. The disposal of sensitive materials **SHOULD** be regulated. All employees **SHOULD** be familiar with these rules. Equipment adequate for disposing of sensitive materials (e.g. file shredders) **SHOULD** be available. Sensitive materials collected for disposal **SHOULD** be protected against unauthorised access.

ORP.1.A10 Response to Violations of Security Policies [Chief Information Security Officer (CISO)]

It **SHOULD** be regulated which reactions will occur if violations of security specifications are suspected. This is the only way to ensure a targeted and prompt response.

ORP.1.A11 Timely Involvement of Employee Representatives [Head of IT]

The Employee Representatives SHOULD be informed promptly of all procedures and projects affecting personnel.

ORP.1.A12 Provisions for Maintenance and Repair Work [IT Operation Department, Building Services, ICS Information Security Officer]

Technical devices SHOULD be maintained at regular intervals. It SHOULD be regulated which security aspects have to be taken into account when performing maintenance and repair work and who is responsible for the maintenance and repair of devices. The employees SHOULD know that maintenance personnel must be supervised when working in-house. The maintenance tasks carried out SHOULD be documented.

ORP.1.A13 Security During Relocations [Head of IT, Head of Building Services, Chief Information Security Officer (CISO)]

Prior to a planned relocation, security policies for this purpose SHOULD be drawn up or updated in good time. All employees SHOULD be informed of the security measures they need to take before, during and after the relocation. During relocation, there SHOULD be a minimum level of site access and system access control. The items transported SHOULD be checked immediately after relocation to ensure they have all arrived undamaged and unmodified.

Requirements in Case of Increased Protection Needs

Generic suggestions for module ORP.1 *Organisation* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

ORP.1.A14 Inspection Rounds [Building Services, Chief Information Security Officer (CISO)] (CIA)

Inspection rounds SHOULD be performed in order to check the extent to which the security specifications are implemented. Instances of negligence that can be easily remedied SHOULD be remedied immediately (e.g. closing windows). Furthermore, causes SHOULD be scrutinised and eliminated.

Additional Information

Currently there is no additional information on threats and security measures for module ORP.1 *Organisation*.

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module ORP.1 *Organisation*:

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.22 Manipulation of Information
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.29 Violation of Laws or Regulations
- G 0.38 Misuse of Personal Information
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.14	G 0.16	G 0.17	G 0.18	G 0.19	G 0.22	G 0.25	G 0.26	G 0.27	G 0.29	G 0.38	G 0.45	G 0.46
ORP.1.A1	X			X	X	X				X	X		X
ORP.1.A2	X	X		X	X	X	X	X	X	X	X		X
ORP.1.A3	X	X			X	X							
ORP.1.A4					X	X				X	X		
ORP.1.A5	X	X			X	X					X		X
ORP.1.A6	X	X			X	X					X		X
ORP.1.A7	X	X		X	X	X	X	X					
ORP.1.A8	X	X		X	X				X				
ORP.1.A9	X				X						X		
ORP.1.A10	X	X	X		X	X	X	X		X	X	X	X
ORP.1.A11				X						X			
ORP.1.A12	X			X	X	X	X	X	X		X		X
ORP.1.A13	X	X		X	X	X	X	X			X		X
ORP.1.A14	X	X			X	X							



ORP.2: Personnel

Description

Introduction

The personnel of a company or a public authority forms the basis for its success or failure. At the same time, the employees are an essential component of information security. Experience has shown that even the most sophisticated security safeguards are ineffective without the proper behaviour of the employees. This essentially requires awareness of what information security means to the organisation and its business processes and the proper way of handling the organisation's information to be protected by the employees.

Objective

The objective of this module is to show which personnel safeguards are to be taken by the human resources department or the supervisors of an organisation to ensure that employees securely treat the information of the organisation and behave according to the security objectives of the organisation and the security requirements of the information to be protected. A number of safeguards are necessary starting from the time the employees are hired and continuing until they leave the organisation. Moreover, other groups of persons coming into contact with the information of the organisation must, of course, not be forgotten, such as employees of service providers and customers. Adequate security safeguards also need to be implemented to handle external personnel, such as visitors, cleaning personnel or maintenance technicians.

Not in Scope

This module covers the requirements which must be observed and fulfilled by the human resources department or supervisors of an organisation. Personnel requirements linked to a specific role, such as the appointment of a system administrator for a LAN, are provided in the modules dealing with the corresponding topic.

Threat Landscape

For module ORP.2 *Personnel*, the following specific threats and vulnerabilities are of particular importance:

Shortage of Personnel

The loss of personnel can cause that certain tasks will not be performed any more or in a timely manner.

Misuse of Authorisation

Everyone who is assigned the task of processing information needs authorisations appropriate for this purpose. Users can misuse these authorisations by exploiting them in order to manipulate or disclose information or otherwise harm the organisation.

Non-Existent or Insufficient Rules

If information security rules are missing, insufficient or cannot be implemented or understood, this can mean the necessary security safeguards are not implemented (see also G 0.29 *Violation of Laws or Regulations*).

Insufficient Knowledge of Rules and Procedures

The specification of rules alone does not ensure they will be followed, nor does it ensure uninterrupted operations. All employees, especially the office managers, must be familiar with the applicable rules. Damage resulting from a lack of knowledge of the existing rules cannot be simply excused by saying "I didn't know I was responsible for that." or "I didn't know what to do".

Misbehaviour

Misbehaviour of persons of all kinds can cause that the confidentiality, integrity or availability of information, business processes or IT systems are impaired. Depending on the protection needs of the information or the systems and depending on the perpetrator's authorisations, the damage can be minor or critical.

Social Engineering

When conducting a social engineering attack, human characteristics such as the willingness to help others, trust, fear or respect for authority are exploited to gain unauthorised access to information or IT systems by "listening in". It can be used to manipulate employees to perform unauthorised tasks.

Carelessness in Handling Information

It can frequently be observed that there are a number of organisational or technical security procedures available in organisations, but they are then undermined through careless handling of the specifications and the technology. A typical example of this includes the almost proverbial sticker on the monitor containing a list of all access passwords.

Unauthorised Use of In-House IT Systems

As a matter of principle, the unauthorised use of employees' own IT systems can only be prevented with difficulty. The use of an employee's own laptops, USB sticks or smartphones within the IT landscape of an organisation can lead to various security risks, such as unintentionally transferring malware.

Abuse of Social Networks

Social networks are very successful as platforms. However, besides various advantages, there are also certain security risks of which the users should not lose sight. Thus, the data published in social networks can be used to skilfully guess passwords. Furthermore, social networks are

particularly suitable for social engineering attacks, since a lot of background information can be collected and the trust assumed among "acquaintances" can be exploited.

Manipulation or Destruction of Equipment, Information or Software

Both external and internal attackers with different motivations may try to manipulate or destroy devices, information or software. The consequences range from unauthorised consultation of sensitive data to the destruction of IT systems, which may lead to significant downtimes.

Requirements

The specific requirements of module *ORP.2 Personnel* are listed below. As a matter of principle, the Human Resources Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	Human Resources Department
Further Roles	Chief Information Security Officer (CISO), IT Operation Department, Supervisor

Basic Requirements

For module *ORP.2 Personnel*, the following requirements **MUST** be implemented as a matter of priority:

ORP.2.A1 Well-regulated familiarisation/training of new employees with their work [Supervisor]

The human resources department as well as the supervisors **MUST** ensure that new employees are familiarised with their new tasks and informed about existing regulations, customs, and procedures at the beginning of their employment. A check list **SHOULD** support this.

As part of the well-regulated familiarisation of new employees, they **MUST** be made aware of existing regulations and instructions for information security. All employees **MUST** be informed about the regulations regarding information security, changes made to them and their specific consequences on a business process or the respective working environment.

All employees **MUST** explicitly be committed to comply with the relevant laws, regulations and internal provisions. Furthermore, all employees **MUST** be informed that all information obtained during work is intended for internal use only unless it is marked otherwise.

ORP.2.A2 Regulated procedure for when employees leave the organisation [Supervisor, IT Operation Department]

Before an employee leaves the organisation, the successor **MUST** be instructed in good time in advance, ideally by the employee leaving the organisation. If a direct handover is not possible, detailed documentation **MUST** be prepared by the employee leaving the organisation. Moreover, all documents, keys and devices as well as ID cards, badges and site-access author-

isations received in connection with their tasks **MUST** be returned by employees leaving the organisation.

The IT administration **MUST** also ensure that all authorisations of former employees to access IT systems are revoked or adapted when employees rotate jobs.

Before the employee leaves the organisation, it **MUST** be explicitly pointed out again that all confidentiality obligations remain in force.

Moreover, business continuity plans and other schedules **MUST** be updated. All the parties affected within the organisation, such as the security personnel, **MUST** also be informed about the employee leaving the organisation. In order to be able to process all the activities associated with the departure of employees in a controlled manner, a check list **SHOULD** be prepared and used, similar to the one used for employees who are hired.

ORP.2.A3 Arrangements for deputies [Supervisor]

The supervisors **MUST** ensure that arrangements for deputies are introduced and maintained. In this respect, it **MUST** be made sure that corresponding and practicable arrangements for deputies are available for all essential business processes and tasks. With respect to these arrangements, the deputy's scope of tasks **MUST** be defined clearly in advance. Here, it is not enough to simply appoint a deputy, it **MUST** be ensured that they have the knowledge required to be a deputy. If this is not the case, it **MUST** be checked how the deputy must be trained or whether it is sufficient to adequately document the current process or project status. If it is impossible in the exceptional case to appoint or train a competent deputy for individual employees, then it **MUST** be determined well in advance whether and, if so, which external personnel could be called in to act as deputies.

ORP.2.A4 Procedures regarding the use of outside staff

When engaging external personnel, they **MUST**, as a matter of principle, be committed to comply with the relevant laws, regulations and internal provisions like all organisation-internal employees. Outside staff who are used for a short time or once can be treated like visitors and **MUST** be supervised in security-relevant areas. If outside staff is engaged for longer periods, however, they **MUST** be instructed regarding their tasks similarly to the organisation's own employees. For these employees, an arrangement for deputies **MUST** also be introduced. When outside staff leaves the organisation, the work results and access authorisations granted, if any, **MUST** be handed over and returned in a controlled manner similarly to the organisation's own personnel.

ORP.2.A5 Non-disclosure agreements regarding the use of outside staff

Before external parties are granted data and site accesses to confidential information, non-disclosure agreements **MUST** be concluded with them. The non-disclosure agreements **MUST** take all important aspects relating to the protection of the organisation's internal information into account.

Standard Requirements

For module ORP.2 *Personnel*, the following requirements correspond to the state-of-the-art technology together with the Basic Requirements. They **SHOULD** be implemented as a matter of principle.

ORP.2.A6 Reviewing applicants when selecting personnel

When selecting new employees, the necessary qualifications and skills SHOULD be worded exactly. Afterwards, it SHOULD be examined on the basis of the documents and in the job interview whether the applicants actually have these qualifications and skills. It SHOULD be ensured in particular that no conflicts of interest arise. In order to avoid conflicts of interest when someone changes positions, non-competition agreements and waiting periods SHOULD be agreed upon.

ORP.2.A7 Verifying the trustworthiness of employees

The trustworthiness of new employees SHOULD be verified before they are hired. Therefore, all parties involved in selecting personnel SHOULD strive with due care and diligence after verifying the applicants' information relevant to assessing their trustworthiness for plausibility to the extent that this is possible. In particular, the curriculum vitae SHOULD critically be checked for completeness, plausibility and correctness. Data that seems critical SHOULD be verified by determined questioning and asking for further proof.

ORP.2.A8 Tasks and responsibilities of employees [Chief Information Security Officer (CISO)]

The tasks and responsibilities of employees SHOULD be documented in a suitable manner, for example by means of employment contracts or agreements. The IT security officer SHOULD ensure that all employees know their tasks and responsibilities in the security process. It SHOULD be agreed in particular that each employees is also responsible for information security after office hours and outside the organisation's premises.

ORP.2.A9 Training of employees

The employees SHOULD receive regular training in their role so that they are always up to date in terms of the activities assigned to them. It SHOULD be ensured in all areas that no employee performs their work based on an outdated level of knowledge. Moreover, the employees SHOULD be given the possibility during their employment to undergo further training within their scope of activities.

All employees SHOULD be instructed in the devices, applications and activities which are used to securely process information. Furthermore, all employees SHOULD regularly be trained in the field of information security and informed about risks and possible countermeasures. The employees SHOULD also be required to independently implement regulations regarding information security. If the training requirements are higher, individual employees SHOULD be trained separately and used as multipliers for the remaining employees within their area of activity.

ORP.2.A10 Avoiding factors impairing the organisational climate

Measures SHOULD also be taken from the perspective of information security to ensure a positive working atmosphere.

Requirement in Case of Increased Protection Needs

Generic suggestions for module ORP.2 *Personnel* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

ORP.2.A11 Analysing the security culture (CIA)

The security safeguards selected for the organisation SHOULD always be orientated to the organisation and its employees. Within the legal framework conditions, there SHOULD be an analysis of exactly how the employees behave from a security perspective. Building on this, there SHOULD be an investigation into where the personnel and organisational security can be improved.

ORP.2.A12 Appointing separate contact persons (CIA)

A person in charge SHOULD be appointed as a trustworthy contact person to contribute to the employees' satisfaction. In the case of major organisational or technical changes, the appointment of such a contact person SHOULD be checked.

ORP.2.A13 Security vetting (CIA)

In the high-security area an additional security vetting for basic verification of the trustworthiness of employees SHOULD be performed.

Additional Information

For more information about threats and security safeguards for module ORP.2 *Personnel*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nist-pubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 15.11.2017

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module ORP.2 *Personnel*:

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.34 Assault

G 0.35 Coercion, Blackmail or Corruption

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0.1 4	G 0.1 6	G 0.1 7	G 0.1 9	G 0.2 2	G 0.2 7	G 0.2 9	G 0.3 2	G 0.3 3	G 0.3 4	G 0.3 5	G 0.3 6	G 0.3 7	G 0.3 8	G 0.4 1	G 0.4 2	G 0.4 4	G 0.4 5	G 0.4 6
ORP.2.A1	X						X							X		X		X	X
ORP.2.A2		X															X	X	X
ORP.2.A3			X				X							X					
ORP.2.A4			X														X	X	X
ORP.2.A5	X	X	X	X	X	X	X	X	X				X	X			X	X	X
ORP.2.A6	X											X				X			
ORP.2.A7		X					X									X		X	X
ORP.2.A8								X									X		
ORP.2.A9				X		X									X	X			
ORP.2.A10					X	X									X				
ORP.2.A11							X			X	X					X		X	X
ORP.2.A12							X												
ORP.2.A13			X						X							X		X	X



ORP.3: Awareness and Training

Description

Introduction

In order to successfully and efficiently implement information security within an organisation, the employees are a necessary and crucial factor for success. All employees must therefore be aware of their roles in information security management. They must know and understand the organisation's security objectives and safeguards and be prepared to support them effectively. To this end, security awareness and a security culture must be established and managed in the organisation.

Employees should be made aware of relevant risks, and they should know how these may affect their organisation. The better the employees understand the threat landscape; the more likely appropriate security measures are to be accepted. Employees should also have the required knowledge to correctly understand and apply safeguards. In particular, they must know what is expected of them in terms of information security and how they should respond in situations critical to security.

Objective

This module describes how to establish and maintain an effective program for raising awareness and conducting training on information security. In the area of information security awareness and training, the aim is to improve employees' perception of security-critical situations and their consequences and give them the necessary knowledge and skills for security-conscious behaviour.

Not in Scope

This module considers requirements for information security awareness and training which relate to the environment within the organisation, as well as to teleworking and mobile working. Employees must receive regular training and be made aware of the relevant information security topics in accordance with the organisation's specifications.

The *ORP.3 Awareness and Training* module describes the process-related, technical, methodological and organisational requirements for information security awareness and training. Other training topics are planned, managed and implemented by the organisation's human resources department or training management department.

In order to avoid redundancies and improve the efficiency of training and continuing education in the organisation, the Chief Information Security Officer should regularly share information not only with the human resources department, but also with the other departments which deal with security (data protection, occupational health and safety, fire safety, etc).

Specific training content for the topics under consideration is set out in many other IT-Grundschrift modules. This module deals with how a systematic, cyclical and organisational approach can be efficiently structured with regard to information security awareness and training.

Threat Landscape

For module ORP.3 *Awareness and Training*, the following specific threats and vulnerabilities are of particular importance:

Insufficient Knowledge of Rules and Procedures

Merely defining rules for information security does not ensure that they will be followed. All employees, and especially office managers, must be familiar with the applicable rules. Although failure to comply with the rules is not the sole cause of many security incidents, it does contribute to the severity of a given situation. Vulnerabilities owing to insufficient knowledge of the rules can pose a threat to the confidentiality, availability, and integrity of the information involved. The performance of tasks and the handling of business processes can be hampered in every respect (e.g. in terms of time, quality, confidentiality) as a result.

Insufficient Awareness of Information Security

Experience has shown that it is not enough to require that certain security measures be implemented. Without an understanding of the reasons for the measures and the purposes they serve, measures often go nowhere or are ignored. If employees are not made sufficiently aware of information security topics, this results in operational and implementation-related risks in the technical and organisational business processes. The security culture, security objectives and security strategy in the organisation can be put at risk if employees cannot perceive a direct connection to their actual working environment because the sense and purpose of security measures is not conveyed. This leads to a lack of acceptance of security measures and shortcomings in compliance.

Unsuccessful Awareness and Training Activities

Activities implemented to raise awareness and provide training are not always as successful as hoped. This may be due to the following:

- Lack of management support
- Unclear objectives
- Poor planning
- Lack of measurement of results
- Lack of continuity
- Insufficient financial or staffing resources

If no appropriate measures are taken in order to ensure the success of the activities implemented, it is often not possible to achieve the objective of the training activity. If the organisation

does not implement sufficient activities for employee awareness and training, aspects of information security can be put at risk, which can lead directly to failures to fulfil tasks.

Insufficient Employee Training Regarding Security Functions

In many cases, employees do not use recently installed security programs and functionalities because they do not know how to operate them and learning how to use them by themselves alongside their daily work routines is considered too time-consuming. Furthermore, a lack of training following the introduction of new software can lead to unintentional operating errors or incorrect configurations. For this reason, it is not enough just to purchase and install (security) software. If employees do not receive sufficient training in software or security functions, they will not be able to work adequately with the IT systems and applications. This can lead to errors in operation and unnecessarily delay work processes. Particularly in critical IT systems and applications, an operating error can result in consequences which threaten the existence of the organisation.

Undetected Security Incidents

Many faults and errors can occur during the day-to-day operation of IT and ICS components. In such cases, there is a risk that security incidents will not be identified as such by the personnel, and that a cyber attack (or related attempts) will thus go undetected. It is sometimes not easy to differentiate between security incidents and technical faults. If users and administrators do not receive specific training in detecting security incidents and reacting appropriately to them, then vulnerabilities can remain undetected and be exploited. If security incidents are not recognised in good time (or at all), appropriate and complete countermeasures cannot be taken in a timely manner. Small vulnerabilities in the organisation can get worse and grow into critical threats to integrity, confidentiality and availability. This can hamper business processes, cause financial damage or lead to regulatory and legal sanctions.

Non-Compliance with Security Measures

For a wide variety of reasons (such as negligence or hectic circumstances), confidential documents can be left out in the open at workstations, emergency exits can be opened from both sides or employees can fail to encrypt e-mails. This can result in damage which otherwise could have been prevented, or at least minimised.

Carelessness in Handling Information

In many cases, there are many organisational or technical security procedures available in organisations, but they are then undermined by careless handling of the specifications and technology involved. A typical example of this involves the almost stereotypical sticker on the monitor listing all the user's access passwords. In the same way, hard disk encryption on a laptop does not stop the person sitting next to you on the train from getting a look at confidential information. The best technological security solutions are no use if print-outs with confidential information are left lying on the printer or end up in freely accessible waste paper bins.

If employees handle information carelessly, the defined information security processes become ineffective. Unauthorised persons can take advantage of negligence in handling information in order to carry out targeted industrial espionage (for example).

Insufficient Acceptance of Information Security

Various circumstances can lead to a lack of acceptance of information security requirements and provisions in an organisation or parts of an organisation, which leads to a lack of understanding of the need to implement security safeguards. This can be due to the culture within the institution that says, "This is the way we've always done it!" or a failure of top management to act as a role model. However, inappropriate or excessive security requirements can also result in employees dismissing security measures. A different social environment or a different cultural background ("When in Rome...") can result in security measures not being implemented, as well. Problems may also arise when certain user rights or even certain hardware or software allocated to a user are viewed as status symbols. Restrictions in these areas may meet with significant resistance.

Social Engineering

Social engineering is a method used to gain unauthorised access to information or IT systems by "listening in" on employees. In social engineering, an attacker generally makes direct contact with a victim (e.g. over the phone, by e-mail, or even on social networks). Attacks using social engineering often comprise several stages. By simulating insider knowledge and, at the same time, appealing to an employee's willingness to help, the attacker can expand their knowledge step by step. If employees are not made sufficiently aware of this type of attack, there is a risk that they will be manipulated into performing unauthorised tasks through skilled persuasion. This may result in them passing on internal information, being infected by malware or even transferring money to purported business partners.

In CEO fraud, clerks who are able to transfer money in the name of the company are misled by instructions from a person pretending to be the CEO. They are told to execute transactions for a supposedly urgent and sensitive deal which is vitally important for the continued existence of the company. Using this scam, con artists managed to inflict millions in damage on thousands of companies in the course of 2016. Calculated globally, the damage runs into the billions.

Requirements

The specific requirements of module ORP.3 *Awareness and Training* are listed below. As a matter of principle, the Chief Information Security Officer is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Human Resources Department, IT Operation Department, Top Management, Supervisor

Basic Requirements

For module ORP.3 *Awareness and Training*, the following requirements **MUST** be implemented as a matter of priority:

ORP.3.A1 Management Awareness of Information Security Issues [Supervisor, Top Management]

The top management **MUST** strongly and actively support security campaigns and training measures for employees. The support of the top management **MUST** therefore be obtained before the beginning of an information security awareness and training program. The top management **MUST** be sufficiently aware of security issues.

All supervisors **MUST** support information security by setting a good example. Managers **MUST** implement the security provisions and emphasise compliance to their employees.

ORP.3.A2 Contact Persons for Security Issues

In every organisation, there **MUST** be contact persons for security issues who can answer both seemingly simple and complex questions. The contact persons **MUST** be known to all employees in the organisation. Related information **MUST** be easily accessible and available to everyone in the organisation.

ORP.3.A3 Employee Instruction in the Secure Handling of IT [Supervisor, Human Resource Department, IT Operation Department]

All employees and external users **MUST** be instructed in and made aware of the secure handling of IT, ICS and IoT components insofar as this is relevant for their work. To this end, binding, clear, up-to-date and accessible policies for the use of the respective components **MUST** be available. If IT, ICS or IoT systems or services are used in a manner which is counter to the interests of the organisation, this **MUST** be communicated.

Standard Requirements

For module ORP.3 *Awareness and Training*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

ORP.3.A4 Designing an Information Security Awareness and Training Program

A targeted awareness and training program **SHOULD** be established for employees. It **SHOULD** be checked and updated regularly.

ORP.3.A5 Target Group Analysis for Awareness and Training Programs

Awareness and training programs **SHOULD** be designed for the appropriate target groups. To this end, target group analysis **SHOULD** be performed so that the measures can be focused on specific requirements and different backgrounds.

ORP.3.A6 Planning and Implementation of Information Security Awareness and Training Measures

All employees **SHOULD** receive information security training according to their tasks and responsibilities. Consequently, there **SHOULD** be awareness and training measures which convey to the employees all of the information and skills which are required in order to be able to implement the security regulations and measures which apply in the organisation. For this reason, the awareness and training content **SHOULD** be structured and planned according to the target groups and the employees' tasks and responsibilities. The planned awareness and training measures **SHOULD** be implemented in an adequate form in accordance with this planning. Awareness and training programs **SHOULD** be reviewed regularly to ensure they are still current, and adapted and developed further if the requirements have changed.

ORP.3.A7 Training in the IT-Grundschutz Methodology

Persons in charge of security SHOULD be familiar with the IT-Grundschutz methodology. If a training requirement has been verified, appropriate IT-Grundschutz training SHOULD be planned and its content should be determined in advance. Within the training, the approach SHOULD be practised using practical examples.

ORP.3.A8 Measurement and Evaluation of Training Success [Human Resource Department]

Success in information security training SHOULD be measured and evaluated according to target groups in order to determine the extent to which the objectives set out in awareness and training programs are achieved. The measurements SHOULD consider both quantitative and qualitative aspects of the awareness and training programs. The results SHOULD be used appropriately to improve the respective awareness and training program.

Requirement in Case of Increased Protection Needs

Generic suggestions for module ORP.3 *Awareness and Training* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

ORP.3.A9 Special Training for Exposed Persons and Organisations (CIA)

Particularly exposed persons, such as functionaries and the employees in particularly exposed organisations or departments of the organisation, SHOULD receive in-depth training with regard to possible threats, appropriate behaviour and precautionary measures.

Additional Information

For more information about threats and security safeguards for module ORP.3 *Awareness and Training*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nist-pubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 15.11.2017

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module ORP.3 *Awareness and Training*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.19 Disclosure of Sensitive Information

G 0.24 Destruction of Devices or Storage Media

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.42 Social Engineering

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.14	G 0.15	G 0.19	G 0.24	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.38	G 0.42	G 0.45	G 0.46
ORP.3.A1	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ORP.3.A2	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ORP.3.A3	X	X	X	X	X	X	X	X	X	X	X	X	X	X
ORP.3.A4					X									
ORP.3.A5					X									
ORP.3.A6					X									
ORP.3.A7	X	X	X	X	X	X	X	X	X	X	X	X	X	
ORP.3.A8					X									
ORP.3.A9	X	X	X	X	X	X	X	X	X	X	X	X	X	X



ORP.4: Identity and Access Management

Description

Introduction

It must be possible to unequivocally identify and authenticate users and IT components which have access to the resources of an organisation. The management of the information this requires is referred to as "identity management".

Access management, meanwhile, defines whether and how users or IT components may access and use information or services (i.e. whether they are granted or refused site, system and data access based on their user profile). Access management includes the processes that are required to assign, withdraw and control rights.

Since these two terms are tightly connected, the term "identity and access management" (IAM) will be used from now on in this module.

Objective

The objective of this module is to ensure that users and IT components can access only the IT resources and information that are required for their work and for which they are authorised, and that no access is granted to unauthorised users and IT components. To this end, it formulates requirements to be used by organisations in establishing secure identity and access management.

Not in Scope

This module describes the basic requirements for implementing identity and access management.

Requirements that relate to components of identity and access management such as operating systems or directory services can be found in the corresponding modules (e.g. SYS.1.3 *Unix Server*, SYS.1.2.2 *Windows Server 2012*, APP.2.1 *General Directory Service*, APP.2.2 *Active Directory*).

Threat Landscape

For module ORP.4 *Identity and Access Management*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Processes in Identity and Access Management

If identity and access management processes are defined insufficiently or not followed, the responsible administrator may not receive information on personnel changes. This can result in the user accounts of former employees not being deleted. They will thus be able to continue accessing sensitive information, or even cloud applications.

It is also possible that employees who move to another department will keep their old authorisations and thereby collect extensive overall authorisations over time.

No Central Means of Deactivating User Access Authorisations

The employees in organisations often have user access authorisations for various IT systems, such as production, test, quality assurance or project systems. In most cases they are located in different areas of responsibility and are managed by different administrators. As a result, identical and unique user IDs are not used on all IT systems and there is no central summary of user access to the individual IT systems in most cases. In such scenarios, it is not possible to immediately deactivate all of an employee's access in case of an attack or password theft. It is also not possible to block all access immediately when an employee leaves the organisation.

Unsuitable Administration of Site, System and Data Access Rights

If the assignment of site, system and data access rights is controlled poorly, this may quickly result in serious security gaps (e.g. due to unchecked growth in assigned rights). When introducing identity management systems or performing audits, it often becomes apparent that various persons in different organisational units are responsible for assigning rights. This quickly results in users being granted authorisations upon request, or only via unnecessarily complicated methods. While the resulting lack of authorisations may impede daily work, granting authorisations when there is no need leads to security risks.

Requirements

The specific requirements of module ORP.4 *Identity and Access Management* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for fulfilling the requirements. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept defined. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Administrator, User, Head of IT

Basic Requirements

For module ORP.4 *Identity and Access Management*, the following requirements **MUST** be implemented as a matter of priority:

ORP.4.A1 Rules for Establishing Users and User Groups [Administrator, Head of IT]

Rules **MUST** be created to define how users and user groups are to be established. All users and user groups **MUST ONLY** be established via separate administrative roles.

ORP.4.A2 Rules for Establishing, Changing and Withdrawing Authorisations [Administrator, Head of IT]

User IDs and authorisations **MUST ONLY** be assigned as actually required. In case of personnel changes, the user IDs and authorisations that are no longer required **MUST** be removed. If employees apply for authorisations that are beyond the standard, they **MUST ONLY** be assigned after additional reasons are cited. All authorisations **MUST** be established via separate administrative roles.

ORP.4.A3 Documentation of Authorised Users and Rights Profiles [Administrator, Head of IT]

Documentation of the authorised users, user groups created and rights profiles **MUST** be produced. The documentation of the authorised users, user groups created and rights profiles **MUST** be checked regularly to ensure they are up to date. The documentation **MUST** be protected against unauthorised access. If the documentation is made available in electronic form, it **SHOULD** be integrated into the backup procedure.

ORP.4.A4 Task Assignment and Segregation of Duties [Head of IT]

The tasks and duties relevant for IT operations **MUST** be defined. The tasks and duties that are not compatible with each other also **MUST** be specified. They **MUST** also be kept separate. They **SHOULD** be documented.

ORP.4.A5 Assignment of Site Access Rights [Head of IT]

It **MUST** be defined which site access rights have been granted to which people in the scope of their respective roles. If site access resources like chip cards are used, their issue and withdrawal **MUST** be documented. Those with site access rights **SHOULD** be instructed as to how to properly handle site access resources. Authorised persons **SHOULD** be blocked temporarily if they are absent for a longer period of time.

ORP.4.A6 Assignment of System Access Rights [Head of IT]

The system access rights that are to be granted to and/or withdrawn from certain people in certain roles **MUST** be defined. If system access resources like chip cards are used, their issue and withdrawal **MUST** be documented. Those with system access rights **SHOULD** be instructed as to how to properly handle system access resources. Authorised persons **SHOULD** be blocked temporarily if they are absent for a longer period of time.

ORP.4.A7 Assignment of Data Access Rights [Head of IT]

It **MUST** be defined which data access rights are to be granted to and/or withdrawn from which people in the scope of their respective roles. If system access resources like chip cards are used, their issue and withdrawal **MUST** be documented. Those with data access rights **SHOULD** be instructed as to how to properly handle system access resources. Authorised persons **SHOULD** be blocked temporarily if they are absent for a longer period of time.

ORP.4.A8 Rules for Password Use [User, Head of IT]

The organisation **MUST** establish mandatory rules for using passwords. They **MUST** specify that only passwords of sufficient length and complexity are to be used. The passwords **SHOULD** be changed at appropriate intervals. The passwords **MUST** be changed immediately if they become known to unauthorised persons (or a corresponding suspicion arises). Passwords **MUST** be kept secret. Default passwords **MUST** be replaced by sufficiently strong passwords and pre-defined logins **MUST** be changed. It **SHOULD** be verified that the allowed password

length is also fully checked by the IT system. In case of unsuccessful login attempts, the system SHOULD not indicate that the password or the user ID is wrong.

ORP.4.A9 Identification and Authentication [Head of IT]

The access to all IT systems and services MUST be protected by appropriate identification and authentication of users, services and IT systems. Pre-configured access resources MUST be changed before production use.

Standard Requirements

For module ORP.4 *Identity and Access Management*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

ORP.4.A10 Protection of User Accounts with Extensive Authorisations [Head of IT]

User accounts with extensive authorisations SHOULD be protected by at least two authentication characteristics.

ORP.4.A11 Resetting Passwords [Head of IT]

An appropriate and secure procedure SHOULD be defined and implemented for resetting passwords. The support staff members that are able to reset passwords SHOULD be trained accordingly. In case of higher password protection needs, a strategy SHOULD be defined for cases in which the support staff member cannot accept responsibility due to the lack of secure options for providing the password.

ORP.4.A12 Developing an Authentication Concept for IT Systems and Applications [Head of IT]

An authentication concept SHOULD be drawn up. This SHOULD include a definition of the functional and security requirements of authentication for each IT system and application. Authentication information SHOULD be transmitted and stored in a cryptographically secure manner.

ORP.4.A13 Suitable Selection of Authentication Mechanisms [Head of IT]

Identification and authentication mechanisms that meet the protection needs SHOULD be used. Authentication data SHOULD be protected by the IT system and/or the IT applications against espionage, modification and destruction during processing.

ORP.4.A14 Checking the Effectiveness of User Separation in the IT System [Administrator]

It SHOULD be checked at reasonable intervals that the users of IT systems log off regularly after completing their tasks and that several users do not use the same ID for their work.

ORP.4.A15 Procedure and Design of Identity and Access Management Processes [Head of IT]

The following processes SHOULD be defined and implemented for identity and access management:

- managing policies

- managing identity profiles
- managing user IDs
- managing authorisation profiles
- managing roles

ORP.4.A16 Policies for Data and System Access Control [Administrator]

A policy for data and system access control SHOULD be drawn up for IT systems, IT components and networks. Standard rights profiles that correspond to the roles and tasks of the employees SHOULD be used. There SHOULD be a written data access rule for every IT system and IT application. Furthermore, all defined uses and assigned rights SHOULD be documented. It SHOULD be ensured that users may only access IT systems and services after having been suitably identified and authenticated.

ORP.4.A17 Suitable Selection of Identity and Access Management Systems [Head of IT]

An identity and access management system SHOULD be appropriate for the organisation and its relevant business processes, organisational structures and processes, as well as its protection needs. The identity and access management system SHOULD be able to map the specifications of the organisation for the handling of identities and authorisations. The identity and access management system chosen SHOULD be suitable for implementing the principle of role separation. The identity and access management system SHOULD be adequately protected against attacks.

ORP.4.A18 Using a Central Authentication Service [Head of IT]

A central authentication service SHOULD be used to establish central identity and access management. The use of a central network-based authentication service SHOULD be planned carefully. To this end, the security requirements relevant in selecting a service of this kind SHOULD be documented.

ORP.4.A19 Instruction of All Employees in the Handling of Authentication Methods and Mechanisms [User, Head of IT]

All employees SHOULD be instructed as to how to properly handle the authentication methods. There SHOULD be comprehensible policies for handling authentication procedures. The employees SHOULD be informed of relevant rules.

Requirements in Case of Increased Protection Needs

Generic suggestions for module ORP.4 *Identity and Access Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

ORP.4.A20 Contingency Planning for the Identity and Access Management System [Head of IT] (CIA)

The extent to which a failed identity and access management system is critical to the security of business processes SHOULD be verified. An authorisation concept SHOULD be available for emergency situations, and there SHOULD be emergency authorisations.

ORP.4.A21 Multi-Factor Authentication [Head of IT] (C)

In case of increased protection needs, secure two-factor or multi-factor authentication (e.g. using cryptographic certificates, chip cards or tokens) SHOULD be used.

Additional Information

For more information about threats and security safeguards for module ORP.4 *Identity and Access Management*, see the following publications, among others:

[29146]	ISO/IEC 29146:2016: Information technology - Security techniques - A framework for access management, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, June 2016
[ISFTS14]	The Standard of Good Practice for Information Security: Area TS2 Cryptography, Information Security Forum (ISF), June 2018
[NIST80053A]	Assessing Security and Privacy Controls in Federal Information Systems: NIST Special Publication 800-53A, particularly areas AC and IA, December 2014

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module ORP.4 *Identity and Access Management*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.44 Unauthorised Entry to Premises

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0.14	G 0.15	G 0.16	G 0.18	G 0.22	G 0.23	G 0.25	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.44	G 0.46
ORP.4.A1				X											
ORP.4.A2				X											
ORP.4.A3				X											
ORP.4.A4					X			X			X		X		
ORP.4.A5			X	X				X						X	
ORP.4.A6				X		X		X							
ORP.4.A7				X		X		X							
ORP.4.A8				X		X		X							
ORP.4.A9	X	X		X	X	X			X		X	X	X		X
ORP.4.A10	X										X	X			
ORP.4.A11				X		X						X			
ORP.4.A12	X										X	X			
ORP.4.A13	X										X	X			
ORP.4.A14				X				X						X	
ORP.4.A15				X											
ORP.4.A16				X											
ORP.4.A17				X					X	X					
ORP.4.A18	X	X		X								X			
ORP.4.A19										X					
ORP.4.A20							X								
ORP.4.A21						X			X		X	X			



ORP.5: Compliance Management

Description

Introduction

In every organisation, there are statutory, contractual, structural and internal rules, regulations and policies from different directions that must be followed. Many of them have a direct or indirect impact on information security management.

The requirements differ depending on the industry, country and other framework conditions. In addition, a public authority (for example) is subject to different external rules and regulations than a public limited company. At the top management level, the organisation must ensure compliance with the requirements and operate a compliance management system.

Depending on the size of an organisation, this system may have different management processes that deal with different aspects of risk management (e.g. security management, data security management, compliance management and controlling). These processes should collaborate in a spirit of trust to exploit synergy effects and avoid conflicts at an early stage.

Objective

The objective of the compliance management module is to illustrate how an overview of the various requirements for the individual areas within an organisation can be established at any time. The module explains how security requirements can be derived from legal, contractual, structural and internal policies and requirements.

Not in Scope

This module considers a selection of requirements which result from legal or contractual provisions and have an impact on the arrangements for information security within the organisation. Sector-specific laws are not addressed.

Threat Landscape

For module ORP.5 *Compliance Management*, the following specific threats and vulnerabilities are of particular importance:

Violation of Laws or Regulations

Insufficient implementation of information security can lead to violations of legal provisions or contractual agreements. Organisations must also comply with a multitude of industry-specific, national and international legal framework conditions. Since these can be very complex,

it is possible for legal provisions to be unintentionally violated, or even intentionally despite one's awareness of the consequences. Example:

- Many cloud service providers offer their services in an international environment. The providers are thus often subject to the laws of different countries. Cloud users, however, often only see low costs and make incorrect assumptions about legal framework conditions that should be taken into account with regard to data protection, information requirements, insolvency law, liability, information access for third parties and other concerns.

Undue Forwarding of Information

Misconduct on the part of individuals can result in sensitive information being passed on without permission. Examples of this include:

- Confidential information being discussed within earshot of outsiders – for example, while talking during a break in a meeting or on a mobile telephone in a public environment
- The supervisor in a department suspects an employee is working together with the competition. In order to prove it, he asks the head of the IT Operation Department to give him "unofficial" access to the employee's e-mails. The head of the IT Operation Department instructs the e-mail administrator to set up this access without obtaining the necessary approval.

Inadequate Checking of the Identity of Communication Partners

Within the framework of personal conversations on the phone or by e-mail, many people are willing to disclose far more information than they would in writing or if more people were present. In so doing, the communication partner is often implicitly expected to treat the contents of the conversations or e-mails as confidential. Furthermore, people tend not to question the identity of communication partners because it is considered impolite. In the same way, permissions are often not sufficiently checked; they are implicitly deduced from a contact's (purported) role instead. Typical examples of this include:

- An employee receives an e-mail from someone who claims to be a contact of their supervisor and explains that the supervisor has agreed to the urgent transfer of an outstanding sum of money.
- A man in a boiler suit with a fitting case gets access to the data centre after he mumbles something about "water pipes".

Accidental Sharing of Internal Information

It is often the case that additional information is inadvertently shared along with the information people intend to send to others. This can result in confidential information falling into the wrong hands. Examples of this include:

- Old files or residual information being shared on storage media; unintended data being transmitted or being transmitted to incorrect recipients.
- In 2015, a French broadcaster was unable to broadcast any programs for hours after a hacker gained access to its internal IT system. In a press conference held after the broadcaster regained the ability to work, a notice board displaying the passwords for all of the possible internal and external IDs was broadcast to the entire world.

Requirements

The specific requirements of module *ORP.5 Compliance Management* are listed below. As a matter of principle, the Compliance Manager is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	Compliance Manager
Further Roles	Persons in Charge of Individual Applications, Chief Information Security Officer (CISO), Human Resources Department, IT Operation Department, Top Management, Head of Organisation, User, Supervisor

Basic Requirements

For module *ORP.5 Compliance Management*, the following requirements **MUST** be implemented as a matter of priority:

ORP.5.A1 Identification of Legal Framework Conditions [Head of Organisation, Top Management]

A process for identifying all relevant legal, contractual and other provisions **MUST** be established within the organisation. All legal framework conditions that affect security management **MUST** be identified and documented.

The legal and contractual provisions which are relevant to the individual departments in the organisation **SHOULD** be presented in detail in a structured overview. The documentation **MUST** be kept up to date. The requirements identified as being security relevant **MUST** be incorporated when planning and designing business processes, applications, and IT systems or when acquiring new components.

ORP.5.A2 Compliance with Legal Framework Conditions [Supervisor, Head of Organisation, Top Management]

Managers who bear the legal responsibility for the organisation on site **MUST** ensure compliance with the statutory provisions. The responsibilities and authorities regarding compliance with statutory provisions **MUST** be defined.

Suitable measures **MUST** be identified and implemented in order to prevent violations of relevant requirements. If violations of relevant requirements are identified, appropriate corrective measures **MUST** be taken in order to ensure compliance.

ORP.5.A3 Employee Obligations to Comply with Relevant Laws, Regulations and Provisions [Supervisor, Human Resources Department]

All employees **MUST** be briefed on relevant laws (e.g. on data protection), regulations and internal provisions and obligated to comply with them. The employees **MUST** know the legal framework that governs their work.

Together with the basic requirements, the following requirements conform to the current state of the art with regard to compliance management. They SHOULD be implemented as a matter of principle.

Standard Requirements

For module ORP.5 *Compliance Management*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

ORP.5.A4 Design and Organisation of Compliance Management [Top Management]

Suitable processes and organisational structures SHOULD be established to ensure an overview of the various legal requirements for the individual departments in the organisation. Persons in charge SHOULD be appointed and their tasks should be determined on the basis of compliance management.

The Compliance Manager and CISO SHOULD work together on a regular basis. They SHOULD integrate security requirements into compliance management, translate security-related requirements into security safeguards and monitor their implementation together.

ORP.5.A5 Granting Exceptions [Supervisor, Chief Information Security Officer (CISO)]

In individual cases, it may be necessary to deviate from specified provisions. Justified exceptions SHOULD be approved by an authorised body following a risk assessment. There SHOULD be an approval procedure for granting exceptions. An overview of the exceptions granted SHOULD be available. An appropriate procedure for documentation and a corresponding review process SHOULD be established. All exceptions SHOULD be granted for a limited period.

ORP.5.A6 Instructing Staff Members in the Secure Handling of IT [Supervisor, Human Resources Department]

All employees and all external IT users SHOULD be instructed in the safe use of the organisation's IT. To this end, they SHOULD be issued binding, clear, current and available policies for the use of IT. These policies SHOULD set out the rights and obligations they have when using IT and the security measures to be taken. The employees SHOULD be notified promptly of changes.

ORP.5.A7 Information Security Continuity [Chief Information Security Officer (CISO)]

To maintain and continuously improve the existing security level, all security safeguards in the security concept SHOULD be regularly reviewed for compliance and necessary improvements. The reviews SHOULD be carried out by internal or external persons who are independent and technically qualified. The results of the reviews SHOULD be documented transparently and presented to the top management. Any shortcomings SHOULD be remedied immediately.

ORP.5.A8 Regular Review of Compliance Management

A procedure SHOULD be established for regular checking of the efficiency and effectiveness of compliance management and the resulting requirements and measures (see also DER.1.3 Audits and Revisions). Regular examination of whether the organisational structure and the processes for compliance management are still appropriate SHOULD be carried out.

Requirements in Case of Increased Protection Needs

Generic suggestions for module *ORP.5 Compliance Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

ORP.5.A9 Protection Against Subsequent Changes to Information [Chief Information Security Officer (CISO), User] (I)

Sufficient security measures SHOULD be taken so that files cannot be changed unnoticed. Depending on the data format and protection needs, suitable methods SHOULD be selected for this. These include, for example, digital signatures and other cryptographic methods, copyright notices or the use of file formats that make subsequent changes and partial processing more difficult. The employees SHOULD be informed of the security mechanisms to be used for this and how they should be used.

ORP.5.A10 Classification of Information (CIA)

There are many departments in an organisation which have higher protection needs or are subject to special restrictions (e.g. regarding personnel-related, financial, confidential or copyright-protected data). Different restrictions apply to the handling of this data depending on how the data is categorised. Consequently, all information SHOULD be classified according to its protection needs and, where possible, labelled accordingly. The employees SHOULD be regularly briefed on the careful handling of information and informed of the restrictions that apply when handling classified data.

ORP.5.A11 Determination of the Legal Framework Conditions for Cryptographic Methods and Products [IT Operation Department, Persons in Charge of Individual Applications] (CI)

Diverse legal framework conditions must be considered when using cryptographic products. The legal framework conditions for the use of cryptographic procedures and products SHOULD be determined and documented for all countries in which they are to be used.

Additional Information

For more information about threats and security safeguards for module *ORP.5 Compliance Management*, see the following publications, among others:

[19600]	ISO 19600:2014: Compliance management systems - Guidelines, International Organization for Standardization (ed.), ISO/TC 309, December 2014
[27002K18]	ISO/IEC 27002:2013: Information technology - Security technique - Code of practice for information security controls, in particular chapter 18 Compliance, International Organization for Standardization (ed.), October 2013

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module *ORP.5 Compliance Management*:

G 0.29 Violation of Laws or Regulations

Elementary Threats Requirements	G 0.29
ORP.5.A1	X
ORP.5.A2	X
ORP.5.A3	X
ORP.5.A4	X
ORP.5.A5	X
ORP.5.A6	X
ORP.5.A7	X
ORP.5.A8	X
ORP.5.A9	X
ORP.5.A10	X
ORP.5.A11	X



CON.1: Crypto Concept

Description

Introduction

The methodology described in this module provides an overview of cryptographic methods and products that may be used in an organisation. It describes how both the data stored locally and that to be transferred can be protected in a heterogeneous environment using cryptographic methods and technologies. Furthermore, suitable organisational and process-related requirements are described that may help guarantee confidentiality, integrity and authenticity.

The present module describes crypto modules. This complements the methods and technologies that may be used to protect locally stored data and transmitted information. The term "crypto module" refers to a product that offers the security functionality specified in the crypto concept. Such products may consist of hardware, software, firmware or a combination thereof. Additionally, components such as memory, processors, buses and power supplies are necessary to implement crypto processes. A crypto module may be used in a wide variety of computer or telecommunication systems in order to protect sensitive data and information. In the present module, this is only relevant for increased protection needs.

Objective

This module describes how information is secured cryptographically in organisations and how a corresponding crypto concept should be drawn up in this regard.

Not in Scope

This module considers general requirements, organisational framework conditions and process-related procedures for cryptographic products and methods. The core IT tasks associated with the operation of crypto modules are not addressed in this module. In this regard, the requirements of the modules of layer OPS.1.1 *Core IT Operations* must be met.

Rather than being covered in the present module, the ways in which individual applications (e.g. e-mails) or IT systems (e.g. laptops) can be secured cryptographically are addressed in the corresponding modules.

Threat Landscape

For module CON.1 *Crypto Concept*, the following specific threats and vulnerabilities are of particular importance:

Inadequate Key Management for Encryption

Inadequate key management may grant attackers access to encrypted data. For example, a lack of rules may result in keys and the associated, encrypted information being stored on the same data storage medium. When symmetrical methods are used, every person who can access the data storage medium or the communication channel in question will thus be able to decrypt the information if the encryption method used is known.

Violation of Legal Framework Conditions Regarding the Use of Cryptographic Methods

If organisations use cryptographic methods and products, they must consider numerous legal framework conditions. In some countries, cryptographic methods may not be used without the consent of the government, for example. This may prevent recipients located abroad from reading the encrypted sets of data because they are not allowed to use the required cryptographic products (which may even make them liable to prosecution).

Furthermore, exporting products with strong encryption is significantly restricted in many countries. It may thus be tempting to leave sensitive data unencrypted or protect it using insecure methods. Besides rolling out the red carpet for attackers, this may also violate national laws. For example, data protection laws may specify that adequate cryptographic methods must be used in order to protect personal data.

Loss of Data Confidentiality or Integrity Due to Misbehaviour

For example, if an organisation uses a crypto module that is either too complicated or not intuitive, the users may dispense with using it for convenience or pragmatic reasons and transfer the information in plain text instead. As a consequence, attackers may eavesdrop on the information transmitted.

An improperly operated crypto module may also result in confidential information being intercepted by attackers – for example, if the information is transmitted in plain text because the plain text mode has accidentally been enabled.

Software Vulnerabilities or Errors in Crypto Modules

Software vulnerabilities or errors in crypto modules weaken the security of the cryptographic methods used and may result in eavesdropping on protected information. As a consequence, it will be possible for attackers to manipulate the crypto modules (e.g. using malware), which can result in leaks of sensitive data or even entire production processes coming to a halt because data can no longer be decrypted.

Failure of a Crypto Module

Crypto modules may fail due to technical defects, power failures or wilful destruction. As a consequence, it may no longer be possible to decrypt data as long as the required crypto module is unavailable. This could result in entire process chains coming to a standstill, e.g. if other IT applications depend on the data.

Insecure Cryptographic Algorithms or Products

Insecure or obsolete cryptographic algorithms can be cracked by a potential attacker using a reasonable amount of resources. In terms of encryption algorithms, this means that an attacker can succeed in converting encrypted text back into the original plain text without hav-

ing to know any additional information, such as the cryptographic key used. If insecure cryptographic algorithms are used, attackers may undermine the cryptographic protection and thereby access sensitive information within the organisation.

Even if only secure (e.g. certified) products are used in an organisation, communications may still become insecure – for example, if a communication partner uses cryptographic methods that do not correspond to the state of the art.

Errors in Encrypted Data or Cryptographic Keys

If information is encrypted and the encrypted data is changed afterwards, the encrypted information might not be decrypted properly. Depending on the mode of operation of the encryption routines, this may mean that only a few bytes are encrypted improperly, or all the data in question. If there is no backup, such data will be lost.

An error in the cryptographic keys used may be even more critical. When a single bit of a cryptographic key is changed, this may already make it impossible to decrypt the data encrypted using the key.

Unauthorised Use of a Crypto Module

If an attacker manages to use a crypto module without being authorised to do so, they may manipulate critical security parameters. As a consequence, the cryptographic methods will no longer provide for sufficient security. Moreover, an attacker may manipulate the crypto module in such a way that it works properly at first glance, but is actually in an insecure condition. This way, the attacker may remain undetected for an extended period of time and access a great deal of sensitive information.

Compromised Cryptographic Keys

The security of cryptographic methods depends to a great extent on how well the confidentiality of the cryptographic keys used is maintained. Therefore, a potential attacker will generally try to determine the keys used. The attacker may succeed in this regard by reading volatile memory or finding unprotected keys that are stored in a backup, for example. If they know the key and the crypto method used, they may decrypt the data relatively easily.

In the case of hard disk encryption (e.g. Trusted Disk), an attacker may position a key logger between a keyboard and a computer in order to obtain the password that is needed to decrypt the hard disk.

Forged Certificates

The purpose of certificates is to link a public cryptographic key to a person. This link between the key and the name of the person is in turn protected cryptographically using a digital signature, which usually comes from a trustworthy neutral organisation.

These certificates are then used by third parties to verify digital signatures of the person identified in the certificate or to provide this person with data encrypted with the key recorded in the certificate.

If such a certificate is forged, false digital signatures will appear to be correctly verified and assigned to the person in the certificate, or data will be encoded and transmitted using a key that may be insecure.

Requirements

The specific requirements of module CON.1 *Crypto Concept* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for compliance with the requirements. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept defined. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	IT Operation Department, Process Owner, Head of IT, Supervisor

Basic Requirements

For module CON.1 *Crypto Concept*, the following requirements **MUST** be implemented as a matter of priority:

CON.1.A1 Selecting Appropriate Cryptographic Methods [Process Owner]

Appropriate cryptographic methods **MUST** be selected. In so doing, it **MUST** be ensured that established algorithms are used that were examined intensively by experts and do not have any known vulnerabilities. The key lengths recommended at the time **MUST** also be used.

CON.1.A2 Backups When Using Cryptographic Methods [IT Operation Department]

In backups, cryptographic keys **MUST** be stored and kept in such a way that unauthorised persons cannot access them. Long-term cryptographic keys **MUST** be stored outside of the IT systems used. In case of long-term storage of encrypted data, it **SHOULD** be checked at regular intervals whether the cryptographic algorithms used and the key lengths still reflect the state of the art. It **MUST** be guaranteed that data stored in encrypted form will still be accessible after longer periods. The crypto products used **SHOULD** be archived. The configuration data of crypto products **SHOULD** be backed up.

Standard Requirements

For module CON.1 *Crypto Concept*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

CON.1.A3 Encryption of Communication Links

It **SHOULD** be checked whether communication links can be encrypted in a feasible manner with a reasonable amount of resources. If this is the case, communication links **SHOULD** be encrypted appropriately.

CON.1.A4 Appropriate Key Management [IT Operation Department, Process Owner]

Cryptographic keys **SHOULD** always be created with appropriate key generators in a secure environment. If possible, cryptographic keys **SHOULD** be used for one purpose only. In particular, different keys **SHOULD** be used for encryption and signature formation.

If keys are used, the authenticity of the origin and integrity of the key data SHOULD be checked.

All cryptographic keys SHOULD be changed at a sufficient frequency. There SHOULD be a defined methodology for scenarios in which a key has been revealed. All created cryptographic keys SHOULD be stored and managed securely.

CON.1.A5 Secure Deletion and Destruction of Cryptographic Keys [IT Operation Department]

Keys and certificates that are no longer needed SHOULD be deleted and destroyed securely. As a general rule, products that do not make it possible to control the storage of the keys SHOULD NOT be used.

CON.1.A6 Identifying the Need for Cryptographic Methods and Products [IT Operation Department, Process Owner]

The tasks for which cryptographic methods are to be used SHOULD be defined. Afterwards, the applications, IT systems and communication links that are necessary to fulfil the tasks SHOULD be identified. These SHOULD be secured cryptographically.

Requirements in Case of Increased Protection Needs

Generic suggestions for module CON.1 *Crypto Concept* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

CON.1.A7 Drawing Up a Security Policy for the Use of Cryptographic Methods and Products (CIA)

Based on the general security policy of the organisation, a specific policy SHOULD be drawn up for the use of crypto products. In the security policy, the person responsible for the secure operation of cryptographic products SHOULD be specified. There SHOULD be rules on how users can stand in for colleagues in relation to the crypto products used.

Necessary training and awareness-raising measures SHOULD be defined for users, along with codes of conduct and reporting channels for potential problems or security incidents. Furthermore, the policy SHOULD define the methods used to ensure that crypto modules are configured securely, used properly and maintained at regular intervals.

The policy SHOULD be known to all relevant employees and SHOULD be the basis of their work. If the policy is changed or deviations prove necessary, this SHOULD be coordinated with the CISO and documented accordingly. Regular checks SHOULD be carried out to determine whether the policy is still implemented properly. The results SHOULD be appropriately documented.

CON.1.A8 Determining the Factors That Influence Cryptographic Methods and Products (CIA)

Before a decision can be taken as to which cryptographic methods and products will be used in the event of high protection needs, the following influencing factors SHOULD be determined (among others):

- security aspects (see CON.1.A6 *Identifying the Need for Cryptographic Methods and Products*)
- technical aspects
- personnel and organisational aspects
- economic aspects
- the lifecycles of cryptographic methods and the key lengths used
- approval of cryptographic products
- legal framework conditions

CON.1.A9 Selecting an Appropriate Cryptographic Product [IT Operation Department, Process Owner] (CI)

Before selecting a cryptographic product, the organisation SHOULD define the requirements to be met by the product. Here, aspects such as the scope of functions, interoperability, efficiency and protection against incorrect operation and malfunction SHOULD be considered. It SHOULD be checked whether certified products should be given priority. The selection process SHOULD also consider the future deployment locations due to the export and import restrictions on cryptographic products (for example).

CON.1.A10 Developing a Crypto Concept (CI)

A crypto concept SHOULD be developed that is integrated into the security concept of the organisation. The concept SHOULD describe all technical and organisational specifications for the cryptographic products used. Additionally, all relevant applications, IT systems and communication links SHOULD be listed. The created crypto concept SHOULD be updated at regular intervals.

CON.1.A11 Secure Configuration of Crypto Modules [IT Operation Department] (CI)

Crypto modules SHOULD be installed and configured securely. All preset keys SHOULD be changed. Afterwards, it SHOULD be tested whether the crypto modules work properly and can actually be operated by the user.

Furthermore, the requirements for the operational environment SHOULD be defined. If an IT system is changed, it SHOULD be tested whether the cryptographic methods used are still effective. The configuration of the crypto modules SHOULD be documented and checked at regular intervals.

CON.1.A12 Secure Separation of Roles When Using Crypto Modules [IT Operation Department] (CI)

User roles SHOULD be defined when configuring a crypto module. Access control and authentication mechanisms SHOULD be used in order to verify whether an employee is actually allowed to use the desired service. The crypto module SHOULD be configured such that the authentication information has to be re-entered every time there is a role change or after a specified period of inactivity.

CON.1.A13 Operating System Security Requirements When Using Crypto Modules (CI)

The interaction between the operating system and the crypto modules SHOULD ensure that the following:

- the crypto modules installed cannot be deactivated or circumvented without this being noticed
- the applied or stored keys cannot be compromised
- the data to be protected can be stored on storage media without encryption or may leave the information-processing system only with the knowledge of and under the control of the user
- attempted manipulations of the crypto module will be detected

CON.1.A14 Training of Users and Administrators [Supervisor, Process Owner, Head of IT] (CIA)

Training measures SHOULD be performed to familiarise the users and administrators with handling the crypto modules they are to operate. The meaning of the security settings of crypto modules and why they are important SHOULD be explained in detail to the users. Furthermore, they SHOULD be made aware of the threats that result from bypassing or disabling these security settings for the sake of convenience. The contents of the training measures SHOULD always be adapted to the particular operational scenarios at hand.

In addition, administrators SHOULD learn how they are to handle resources for verifying cryptographic settings. They SHOULD also be provided with an overview of basic cryptographic terms.

CON.1.A15 Reacting to the Practical Weakening of a Crypto Method (CI)

A process SHOULD be established that may be used in the event of a weakened cryptographic method in order to guarantee the information security of the organisation. In so doing, it SHOULD be ensured that the weakened cryptographic method can be secured or will be superseded by an appropriate alternative.

CON.1.A16 Physical Security of Crypto Modules [Head of IT] (CI)

Unauthorised physical access to the contents of a crypto module SHOULD be prevented. Hardware and software products used as crypto modules SHOULD be able to perform a self-test.

CON.1.A17 Emission Security [Head of IT] (C)

It SHOULD be examined whether additional safeguards regarding emission security are necessary. This SHOULD be considered particularly important when processing official material (VS) that is classified as VS-CONFIDENTIAL or higher.

CON.1.A18 Cryptographic Replacement Modules [Head of IT] (CIA)

Replacement crypto modules SHOULD be kept in stock.

Additional Information

For more information about threats and security safeguards for module CON.1 *Crypto Concept*, see the following publications, among others:

[27001A10]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, in particular Annex A, A.10 Cryptography, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[BSILEK]	Leitfaden Erstellung von Kryptokonzepten [Guidelines for Creating Crypto Concepts]: Federal Office for Information Security (BSI), Version 1.0, July 2008, https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/Arbeitshilfen/Kryptokonzept/Kryptokonzept_node.html , last accessed on 05.10.2018
[BSIMKK]	Musterkryptokonzept [Crypto Concept Model]: Federal Office for Information Security (BSI), Version 1.2, April 2010, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Krypto/2010-04-28_Musterkryptokonzept_V12_pdf.pdf , last accessed on 05.10.2018
[ISFTS2]	The Standard of Good Practice for Information Security: Area TS2 Cryptography, Information Security Forum (ISF), June 2018
[NIST800175 B]	Guidelines for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms, NIST Special Publication 800-175B, August 2016, https://csrc.nist.gov/publications/drafts/800-175/sp800-175b_draft.pdf , last accessed on 05.10.2018
[TR02102]	Cryptographic Mechanisms: Recommendations and Key Lengths: BSI TR-02102, Federal Office for Information Security (BSI), January 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , last accessed on 13.09.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module CON.1 *Crypto Concept*:

G 0.13 Interception of Compromising Interference Signals

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.37 Repudiation of Actions
- G 0.40 Denial of Service
- G 0.43 Attack with Specially Crafted Messages
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0.1 3	G 0.1 4	G 0.1 5	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 5	G 0.2 6	G 0.2 7	G 0.2 8	G 0.2 9	G 0.3 0	G 0.3 1	G 0.3 2	G 0.3 7	G 0.4 0	G 0.4 3	G 0.4 5	G 0.4 6
CON.1.A1		X	X	X				X						X				X		X		
CON.1.A2		X	X												X						X	X
CON.1.A3		X	X																			X
CON.1.A4		X	X	X	X			X							X							X
CON.1.A5		X	X		X	X		X							X							
CON.1.A6				X																		
CON.1.A7				X	X							X				X						
CON.1.A8				X										X								
CON.1.A9		X	X	X				X	X				X	X	X			X				X
CON.1.A10				X																		
CON.1.A11		X	X	X	X	X	X	X														
CON.1.A12								X						X	X	X	X					X
CON.1.A13					X	X	X	X														
CON.1.A14					X											X						
CON.1.A15				X										X								
CON.1.A16							X	X			X				X							
CON.1.A17	X	X	X																			



CON.2: Data Protection

Description

Introduction

Data protection is designed to protect individuals so that the use of personal data by organisations does not affect their fundamental rights. The constitution of the Federal Republic of Germany includes citizens' fundamental right to decide how their personal data is used. The federal and state data protection laws refer to this when they highlight the protection of the right to informational self-determination. In Article 8, the EU Charter of Fundamental Rights directly describes the right to protection of personal data (paragraph 1), highlights the necessity of a legal basis for data processing (paragraph 2) and prescribes the monitoring of compliance with data protection regulations by an independent body (paragraph 3). The General Data Protection Regulation [GDPR] provides more details on such requirements of the Charter of Fundamental Rights. Article 5 of the GDPR, which states the basic principles that are partially identified as *protection goals*, is of extraordinary importance in this regard. The German Standard Data Protection Model (SDM) offers a method for systematic monitoring of this required implementation of data protection regulations on the basis of seven data protection goals / goals of guaranteeing.

Objective

The aim of this module is to show the connection between the requirements of the German Standard Data Protection Model and IT-Grundschutz.

Not in Scope

The conference of the independent federal and state data protection agencies developed the German Standard Data Protection Model as a concept that systematises the technical and organisational measures stated in the German and European legal regulations on the basis of data protection goals / goals of guaranteeing. On the one hand, the model is used by bodies responsible for processing to systematically plan and implement required measures and thereby promote the design and organisation of IT methods and applications in accordance with data protection. On the other hand, the model offers the data protection agencies a way to render a transparent, comprehensible and robust overall assessment of a given method and its components using a uniform system. As a method, the SDM is suitable for regularly checking, assessing and evaluating the effectiveness of the technical and organisational measures of processing on the basis and in accordance with the criteria of the GDPR.

When selecting appropriate technical and organisational measures, the SDM adopts the perspective of data subjects in asserting their fundamental rights, which is why it differs significantly from the viewpoint of IT-Grundschutz. IT-Grundschutz primarily focuses on information security and protecting organisations that process data. In the SDM, on the other hand,

measures are selected based on the impairment that data subjects must accept as a result of the organisation's data processing activities.

Given this background, the selection of measures for guaranteeing information security for organisations by responsible bodies is to be differentiated from the selection of measures for guaranteeing the rights of data subjects. The IT-Grundschrift Methodology is primarily designed to ensure information security, while the German Standard Data Protection Model is meant to uphold the rights of data subjects.

The German Standard Data Protection Model thus seeks to fulfil the following standards:

- It transfers requirements under data protection law into a catalogue of data protection goals / goals of guaranteeing.
- It divides the considered methods into three components: data, IT systems and processes.
- It considers the categorisation of data into three levels of information security requirements – normal, high, and very high – and supplements this classification with corresponding considerations at the level of processes and IT systems.
- On this basis, it offers a systematically derived catalogue that includes standardised protection measures.

Threat Landscape

For module CON.2 *Data Protection*, the following specific threats and vulnerabilities are of particular importance:

Non-Compliance with Data Protection Laws or Use of an Incomplete Risk Model

According to the EU General Data Protection Regulation, the processing of personal data is basically forbidden and requires a legal basis. Collecting, using and transferring personal data is only admissible if this is allowed for or ordered by a statutory provision, or if the data subject has given consent (see Article 6 [GDPR]).

From the perspective of data protection, an organisation that collects, uses, transfers or receives (in summary: "processes") personal data is fundamentally a risk for individuals. This risk will not change if the data processing of an organisation is legally compliant.

An even greater risk exists for persons if an organisation does not process data for a sufficiently specific purpose; makes the purpose too broad; or carries out the processing completely without purpose, in a non-transparent manner, or with no measures to ensure integrity or sufficient intervention options for data subjects.

In practice, third-party access that does not serve the purpose of the original data processing can represent a frequent risk. In typical cases, this may involve foreign parent companies, security agencies, banks and insurance companies, public service administrations, IT manufacturers and IT service providers (for example, when patient and client directories are handed over) or research organisations. In these contexts, the appropriateness of access is often not checked. This can be because a practice that has been in place for many years is continued, for example, or because subordinate employees shy away from the personal risk that can lie in addressing the existence of a sufficient legal basis. Furthermore, (partially) negative results of

checks by a legal department or a data protection officer often do not result in corresponding action being taken by the persons in charge.

Another risk to both persons and responsible organisations can arise from a lack of standard processes for (mainly only conditional) access to IT services or the transmission of data pools for legitimate access by third parties, or if no proof regarding the appropriateness of such access can be provided by means of logs and documentation.

Inappropriate data security poses a large risk to persons. Recital 75 of the GDPR describes the risks associated with the processing of personal data and thus the threat posed by unauthorised access as follows: “The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.”

Definition of Insufficient Protection Needs

The definition of insufficient protection needs poses another risk to individuals. Incorrectly assessed protection needs result in non-adherence to essential requirements in designing the functions of a procedure in line with the data protection laws and the application of specific data protection measures. The protection needs typically defined by an organisation which processes personal data itself in a responsible manner can be inaccurate or insufficient from the perspective of individuals for various reasons:

- The organisation did not take into account the catalogue of data protection goals that extends beyond information security.
- When determining the protection needs, the organisation did not distinguish between the risks regarding the implementation of data subjects' fundamental rights and the risks to the organisation.
- Although the organisation has distinguished between the two protection interests, it has designed the functions of the procedure and the protection measures in favour of the organisation or to the disadvantage of data subjects.

Requirements

The specific requirements of module *CON.2 Data Protection* are listed below. As a matter of principle, the Data Protection Officer is responsible for monitoring compliance with the requirements of GDPR (for details and restrictions, see Art. 39 GDPR). The Chief Information Se-

curity Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are fulfilled and verified according to the security concept defined.

Module Owner	Data Protection Officer
Further Roles	

Basic Requirements

For module CON.2 *Data Protection*, the following requirements **MUST** be implemented as a matter of priority:

CON.2.A1 Implementing the German Standard Data Protection Model

It **MUST** be checked that the German Standard Data Protection Model (SDM) is being used. Any instance in which the complete catalogue of protection goals is not considered or the SDM methodology and reference measures are not used **MUST** be justified.

Standard Requirements

For module CON.2 *Data Protection* there are no *Standard Requirements*.

Requirements in Case of Increased Protection Needs

For module CON.2 *Data Protection* there are no Requirements in Case of Increased Protection Needs.

Additional Information

For more information about threats and security safeguards for module CON.2 *Data Protection*, see the following publications, among others:

[DSGVO]	EU General Data Protection Regulation: “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”, April 2016, http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679 , last accessed on 23.07.2018.
[SDM]	Das Standard-Datenschutzmodell (SDM) - Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungszielen [The Standard Data Protection Model (SDM)- A Method for Data Protection Consulting and Auditing on the Basis of Uniform Data Protection Goals]: AK Technik der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (ed.), V1.0 Erprobungsfassung, November 2016, https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html , last accessed on 23.07.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module CON.2 *Data Protection*:

G 0.18 Poor Planning or Lack of Adaptation

Elementary Threats Requirements	G 0.18
CON.2.A1	X



CON.3: Backup Concept

Description

Introduction

As companies and public agencies store more and more data, they are becoming increasingly dependent on it, as well. If data is lost (e.g. due to defective hardware or malware), this may result in serious damage. However, such effects can be minimised by means of regular backups. A backup is intended to guarantee that IT operations can be resumed quickly by means of a redundant set of data if parts of the operative data set are lost.

Objective

This module shows how organisations can draw up a backup concept and which requirements should be considered.

Not in Scope

The module describes the basic requirements that help ensure an appropriate backup concept. Requirements for the long-term storage and maintenance of electronic documents are not addressed. These are included in module OPS.1.2.2 *Archiving*. This module does not address system-specific or application-specific requirements for logging; these are included in the relevant modules of the IT-Grundschutz Compendium, e.g. SYS.1.1. *General Server*, APP.3.2 *Web Servers*, or NET.3.2 *Firewall*.

Threat Landscape

For module CON.3 *Backup Concept*, the following specific threats and vulnerabilities are of particular importance:

Lack of Backups

Organisations increasingly depend on their IT systems and the data stored on them. If data is lost (e.g. due to malware, technical malfunction, fire or intentional or inadvertent deletion by employees) and no backup is present, the resulting damage can threaten the existence of the organisation – for example, if all customer data is lost.

Lack of Recovery Tests

An organisation regularly backs up its most important data – above all, its customer data. However, if tests are not performed regularly as to whether data can be recovered, the backed-up data could be unusable if recovery is then required. In the case of customer data, this could result in significant damage to the organisation, and possibly in a discontinuation of distribution.

Inappropriate Storage of Backup Media

Backup storage media contain a large amount of an organisation's sensitive information. If the storage media are stored at an insecure location, an attacker (within the organisation, for example) may access them and steal or manipulate sensitive information. Backup storage media can also become unusable due to inappropriate storage or room climate conditions, rendering them unavailable when needed.

Non-Existent or Inappropriate Documentation

If backup measures are not documented or only documented insufficiently, recovery may take more time than planned. This may result in delays to important processes, e.g. in production. It is also possible that a backup cannot be recovered at all and the data is thus lost.

Non-Compliance with Statutory Regulations

If statutory regulations (e.g. data protection laws) are not complied with in connection with backups, organisations may be required to pay fines or damages.

Insecure Cloud Providers

If organisations outsource their backups to a cloud provider, an attacker could access the backup files or it may not be possible to restore them with the required speed. This may result in sensitive data being read or backups not being available in due time.

Insufficient Storage Capacities

The amount of data being processed (and thus stored) is constantly increasing. If the backup media do not have sufficient storage space, the most current data will no longer be backed up or the employed backup software will automatically overwrite backups that are older, but still needed. If the persons in charge are not aware of this (e.g. due to insufficient monitoring), data may be lost completely or the wrong versions may be the only ones available in an emergency.

Inappropriate Backup Concept

If no appropriate backup concept is created and complied with for backup measures, it will not be possible to recover backed-up data if required. Since most backed-up data constitutes sensitive information, backups need to be encrypted. If a loss of data also affects the key for decrypting a backup because the need to store such keys separately was not considered, recovery might not be possible.

Requirements

The specific requirements of module CON.3 *Backup Concept* are listed below. As a matter of principle, the Chief Information Security Officer is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	IT Operation Department, Process Owner, Head of IT

Basic Requirements

For module CON.3 *Backup Concept*, the following requirements MUST be implemented as a matter of priority:

CON.3.A1 Determining the Factors That Influence Backups [Process Owner, IT Operation Department]

The relevant influencing factors – such as change volumes, change times and availability and integrity requirements – MUST be determined for every IT system and (if applicable) for individual IT applications of particular importance. To this end, the administrators and the persons in charge of the individual IT applications SHOULD be consulted. The results MUST be recorded in a clear and appropriate manner. New requirements MUST be taken into consideration promptly in an updated backup concept.

CON.3.A2 Stipulating Backup Procedures [Process Owner, IT Operation Department]

A method of backing up data MUST be specified for every IT system and every data type. To this end, the type, frequency and points in time of backups MUST be defined. In addition, the responsibilities for the backups MUST be defined. The storage media to be used and the required transport and storage modalities MUST also be defined.

CON.3.A3 Determining Legal Factors That Influence Backups

The legal requirements for backups MUST be determined and included in the minimum and/or in the backup concept.

CON.3.A4 Drawing Up a Minimum Backup Concept

A minimum backup concept specifying the minimum requirements to be complied with regarding backups MUST be drawn up. This includes short descriptions on how to create and recover backups, which parameters have been selected, and which hardware and software are used.

CON.3.A5 Regular Backups [IT Operation Department]

Backups MUST be performed regularly. At minimum, the data that cannot be derived from other information MUST be backed up regularly. The backups created MUST be suitably protected against third-party access. Tests MUST be performed regularly to determine if the backup functions as desired. In particular, such tests MUST determine if the data backed up can also be restored without any problems.

Standard Requirements

For module CON.3 *Backup Concept*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

CON.3.A6 Developing a Backup Concept [Process Owner, Head of IT]

A backup concept SHOULD be created. This SHOULD be agreed with all the persons in charge. This SHOULD include all the IT systems to be considered. The employees SHOULD be informed of the parts of the backup concept that apply to them. It SHOULD be checked regularly whether the backup concept is still being implemented properly.

CON.3.A7 Procuring a Suitable Backup System [IT Operation Department, Head of IT]

Before procuring a backup system, a requirements list SHOULD be drawn up that can be used to evaluate the products available on the market. The backup systems purchased SHOULD meet the requirements of the security and backup concept.

CON.3.A8 Functional Tests and Verification of Recoverability [IT Operation Department]

Tests SHOULD be performed regularly to determine if the backup process is working as desired, and in particular if the data backed up can also be restored without any problems and within an appropriate period of time.

CON.3.A9 Prerequisites of Online Backups [IT Operation Department, Head of IT]

If online storage is to be used for backups, at least the following SHOULD be regulated:

- the formulation of the contract
- the data storage location
- service level agreements (SLAs)
- appropriate authentication methods
- data encryption
- transport encryption

CON.3.A10 Employee Obligations Regarding Backups

All employees SHOULD be informed of the regulations on backups. They SHOULD also be informed of the tasks they are obliged to carry out in creating backups.

CON.3.A11 Backup Copies of Software in Use [IT Operation Department]

Backup copies of the software programs used SHOULD be made whenever this is legally allowed and technically possible. In this regard, all the packages and information necessary to quickly reinstall the software in an emergency SHOULD be available. The original installation sources and the licence numbers SHOULD be stored at a secure location.

CON.3.A12 Suitable Storage of Backup Media [IT Operation Department]

The backup storage media SHOULD be protected against unauthorised access. They SHOULD be stored in a place that is separate from the source systems. The storage location SHOULD have a climate that allows for long-term storage of the storage media.

Requirements in Case of Increased Protection Needs

Generic suggestions for module CON.3 *Backup Concept* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

CON.3.A13 Using Cryptographic Methods for Backups [IT Operation Department] (CIA)

All data SHOULD be encrypted to ensure the confidentiality and integrity of backup data. It SHOULD be ensured that the encrypted data can be restored even after longer periods. The cryptographic keys used SHOULD be protected by a separate backup.

Additional Information

For more information about threats and security safeguards for module CON.3 *Backup Concept*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[BKBU]	Backup / Recovery / Disaster Recovery Guidelines: Federal Association for Information Technology, Telecommunications and New Media (Bitkom), December 2016, https://www.bitkom.org/noindex/Publikationen/2017/Leitfaden/170125-LF-Backup-Recovery.pdf , last accessed on 05.10.2018
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nist-pubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 15.11.2017

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module CON.3 *Backup Concept*:

G 0.2 Unfavourable Climatic Conditions

G 0.4 Pollution, Dust, Corrosion

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.2	G 0.4	G 0.14	G 0.18	G 0.19	G 0.22	G 0.25	G 0.26	G 0.28	G 0.29	G 0.31	G 0.45	G 0.46
CON.3.A1			X		X		X			X		X	X
CON.3.A2				X									
CON.3.A3			X		X		X			X		X	X
CON.3.A4				X									
CON.3.A5				X		X							
CON.3.A6				X									
CON.3.A7										X			
CON.3.A8							X	X	X				
CON.3.A9				X			X	X			X	X	
CON.3.A10				X								X	X
CON.3.A11										X		X	
CON.3.A12	X	X				X	X					X	
CON.3.A13				X		X						X	



CON.4: Selection and Use of Standard Software

Description

Introduction

Standard software refers to software that is offered on the market and mainly purchased from specialist retailers, e.g. via catalogues or online portals. It is characterised by the fact that organisations install it themselves and can adapt it with little effort.

This module shows how organisations should handle standard software considering the relevant security aspects. Organisations must draw up a requirements catalogue for standard software, select a suitable product, install it in a secure manner, manage the licences appropriately, and be able to securely uninstall the product.

Objective

This module systematically shows the security safeguards to be taken so that standard software can be planned, purchased, operated and discarded in a secure manner. The primary objective is to protect the information processed with the standard software.

Not in Scope

This module only addresses standardised programs that are designed for use and adaptation by users themselves without requiring support from the manufacturer or external service providers.

The present module does not address software tests or approvals. Related requirements are included in OPS.1.1.6 *Software Tests and Approvals*. Software development is also not addressed. In this regard, the requirements of module CON.8 *Software Development* should be considered separately.

Detailed information on disposal is included in module OPS.1.2.6 *Sale and Disposal of IT*. Further requirements for cloud applications are included in the modules OPS.2.2 *Cloud Usage* and APP.1.3 *Cloud Applications from a Client Perspective*.

Threat Landscape

For module CON.4 *Selection and Use of Standard Software*, the following specific threats and vulnerabilities are of particular importance:

Lack of Adaptation of Standard Software to the Needs of the Organisation

If purchased standard software is not adapted to the requirements of the organisation, internal operations can be significantly impaired. For example, formats can be incompatible with programs already in use, or the scope of functions of new products could be insufficient. This may result in performance losses, malfunctions or errors within business processes.

Disclosure of Sensitive Information Due to Incorrect Configuration

If standard software is configured incorrectly, e.g. if functions not required are still activated, sensitive information could be inadvertently disclosed. This may result in financial losses or damage to the organisation's reputation. In addition, the organisation could also violate applicable laws, e.g. by disclosing personal data.

Purchasing Standard Software and Updates from an Unreliable Source

If standard software or relevant updates are purchased from unreliable sources, the integrity and functionality of the software cannot be guaranteed. This also applies to extensions (*plug-ins* or *add-ons*). The installation of compromised software may result in malware being distributed within the organisation and the software not working as intended. Moreover, the integrity and availability of IT systems can be impaired.

Manipulation of Data by Users

The data used in standard software can be manipulated by users in a variety of ways, e.g. if they enter data incorrectly by mistake, deliberately change its content or simply delete it. This will impair all the specialised processes for which the relevant application is used. If manipulated data is not detected, falsified information will be processed. Furthermore, this may result in vulnerabilities that can be exploited by attackers.

Software Vulnerabilities or Errors in Standard Software

Despite intensive testing, it is often the case that not all vulnerabilities and errors can be detected in standard software before it is delivered to customers. If they are not detected in time, the resulting crashes or errors can have serious consequences. Furthermore, the confidentiality and integrity of the stored data, as well as the availability of affected IT systems, can be impaired. Software deficiencies and/or errors may also result in serious vulnerabilities in standard software. Under certain circumstances, they can be exploited by attackers to smuggle in malicious code.

Using Unlicensed Standard Software

If standard software is used without a valid software licence, e.g. because the licence volume has been inadvertently exceeded, this may result in contractual penalties. By the same token, the licence costs may be too high if standard software is installed on workstations that do not require it.

Misuse of Rights in Standard Software

Site, system and data access rights are used as organisational safeguards to protect information, business processes and IT systems against unauthorised access. If unauthorised persons are able to use standard software or certain functions, they may be able to threaten the confidentiality and integrity of information by changing, deleting or improperly creating it. The improper assignment of rights is one factor that can cause such vulnerabilities. Affected business

processes can be corrupted, inadvertently process incorrect information, or disclose sensitive information.

Data Loss Due to Incorrect Use of Standard Software

Incorrect use of standard software may result in employees inadvertently deleting or changing data and rendering it unusable. This may block entire business processes. Incorrect use of encryption functions may also make it impossible to decrypt data. In this instance the data cannot be recovered or can only be recovered at an increased cost, which can be an additional financial burden on the organisation.

Requirements

The specific requirements of module *CON.4 Selection and Use of Standard Software* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept defined. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Department, Procurement Department

Basic Requirements

For module *CON.4 Selection and Use of Standard Software*, the following requirements **MUST** be implemented as a matter of priority:

CON.4.A1 Guaranteeing the Integrity of Standard Software

When installing standard software, it **MUST** be ensured that the program is original and unchanged. To this end, it **MUST** be installed from either original media or verified identical copies of the original installation program. Access to the installation routines **MUST** be restricted to authorised employees. The original storage media or the installation program **MUST** be checked for malware. Backup copies of the installation files **SHOULD** be created and checked.

CON.4.A2 Developing Installation Instructions for Standard Software

Installation instructions **MUST** be drawn up for the standard software selected. Suitable configuration parameters and organisational framework conditions for installation of the software **MUST** be specified.

CON.4.A3 Secure Installation and Configuration of Standard Software

Approved standard software **MUST** be installed and configured in accordance with the corresponding installation instructions (see *CON.4.A2 Developing Installation Instructions for Standard Software*). If the instructions are not followed, this **MUST** be approved by the Supervisor. All installations **MUST** be performed by the IT Operation Department. Here, it **MUST** be ensured that only the required program functions are installed.

The software **MUST** be configured so that it meets the security policy of the organisation. Services and functions that are not required **MUST** be uninstalled. If this is not possible, they **MUST** be deactivated. Before and after installing standard software, all the IT systems involved **SHOULD** be backed up.

Standard Requirements

For module CON.4 *Selection and Use of Standard Software*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

CON.4.A4 Determining Responsibilities Regarding Standard Software [Department]

Those responsible for implementing standard software **SHOULD** be appointed. This **SHOULD** at least determine who is responsible for drawing up a requirements catalogue, selecting a product, testing and approving the product, and installing it. In addition, an implementation and approval process **SHOULD** be defined. Technical Product Owners **SHOULD** be appointed to operate standard software.

CON.4.A5 Drawing Up a Requirements Catalogue for Standard Software [Department]

Before purchasing standard software, a requirements catalogue containing both functional and security requirements **SHOULD** be drawn up. To this end, the program requirements of the specialised and IT departments **SHOULD** be collected. The requirements catalogue **SHOULD** be finalised with all the departments involved.

CON.4.A6 Selecting Appropriate Standard Software [Department, Procurement Department]

The products available on the market **SHOULD** be examined on the basis of the requirements catalogue (see CON.4.A5 *Drawing Up a Requirements Catalogue for Standard Software*) and **SHOULD** be compared using a rating scale. Accordingly, it **SHOULD** be examined whether the products on the short list actually meet the requirements of the organisation. If there are several product alternatives, additional effort (e.g. for training or migration) **SHOULD** be considered. Finally, the Procurement Department **SHOULD** work with the head of the department making the request and the IT Operation Department on selecting an appropriate software product based on the evaluations and test results.

CON.4.A7 Checking the Delivery of Standard Software [Department]

It **SHOULD** be checked that new software products have been delivered completely and correctly. At minimum, it **SHOULD** be checked whether the delivery was actually ordered, for whom it is intended, and whether all the required components are present. Software that is only available for download **SHOULD** be subject to corresponding checks, along with the relevant licence files or keys. The results of the checks **SHOULD** be documented. All delivered products and licence information **SHOULD** then be assigned unique identifiers and added to an inventory list.

CON.4.A8 Licence Management and Version Control for Standard Software

Standard software products that require a licence and are used on IT systems of the organisation **SHOULD** be licensed. In order to ensure this, the installed program versions and their licences **SHOULD** be checked regularly. In this regard, corresponding lists, databases or particular licence management programs **SHOULD** be used. The inventory lists for the licences

SHOULD always be up to date. In addition, the various configurations of the standard software installed SHOULD be documented.

CON.4.A9 Uninstalling Standard Software

The uninstallation of standard software SHOULD remove all files created for operation of the software on the corresponding IT system. In addition, all the entries made in system files for the product SHOULD be deleted. The system changes made during installation SHOULD be documented either manually or using corresponding programs in order to completely uninstall standard software.

Requirements in Case of Increased Protection Needs

Generic suggestions for module *CON.4 Selection and Use of Standard Software* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

CON.4.A10 Implementing Additional Security Functions (CIA)

It SHOULD be checked that the security functions of the standard software in use are appropriate for increased protection needs. If this is not the case, suitable functions SHOULD be implemented in order to safeguard operations.

In principle, increased protection needs SHOULD already be considered when defining requirements and selecting a product.

CON.4.A11 Using Certified Standard Software (CIA)

When purchasing standard software, it SHOULD be determined whether the assurances of the manufacturer, distributor or provider regarding the security functions implemented can be considered to be sufficiently trustworthy. If this is not the case, a certification of the application according to the Common Criteria SHOULD be factored into the selection process. If several products are available, security certificates SHOULD be considered, particularly if the evaluated scope of functions includes the minimum functions (or most of them) and the strength of the corresponding mechanisms matches the protection needs at hand. If no suitable and certified product is available on the market, the environment in which the standard software is to be used SHOULD be safeguarded in accordance with high protection needs.

CON.4.A12 Using Encryption, Checksums or Digital Signatures (CI)

When transmitting or storing data with increased protection needs, the data SHOULD be encrypted in advance. If standard software has an integrated encryption function, it SHOULD be checked that it is sufficiently secure. This SHOULD be checked in cases involving older product versions in particular. Users SHOULD be trained and made aware of how to handle encryption functions.

Additional Information

For more information about threats and security safeguards for module *CON.4 Selection and Use of Standard Software*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[CC]	Common Criteria for Information Technology Security Evaluation (CC): (see also ISO/IEC 15408-2:2008 ISO, Information technology - Security techniques - Evaluation criteria for IT security), www.commoncriteriaportal.org , last accessed on 24.08.2018
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nist-pubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 15.11.2017
[TR02102]	Cryptographic Mechanisms: Recommendations and Key Lengths: BSI TR-02102, Federal Office for Information Security (BSI), January 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , last accessed on 13.09.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module CON.4 *Selection and Use of Standard Software*:

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.22 Manipulation of Information

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.18	G 0.19	G 0.20	G 0.22	G 0.28	G 0.29	G 0.30	G 0.31	G 0.45	G 0.46
CON.4.A1							X			X
CON.4.A2								X		
CON.4.A3	X	X						X		
CON.4.A4							X			
CON.4.A5						X			X	X
CON.4.A6	X									
CON.4.A7			X		X					
CON.4.A8						X				
CON.4.A9		X						X		
CON.4.A10				X					X	X
CON.4.A11	X									
CON.4.A12		X		X			X		X	X



CON.5: Development and Use of Generic Applications

Description

Introduction

Specialised applications are complex applications that are designed for individual and specific technical tasks and are usually not purchased and used as standard solutions. Instead, basic solutions are adapted for the individual intended purposes of organisations, or the applications are developed completely by third parties (or the organisation itself). Such specialised applications include personnel management software or procedures for managing social data or reporting data. Careful planning of security safeguards before selecting and commissioning an application is essential for the security level achieved because it is difficult to compensate for errors in planning (e.g. a lack of security functions) during live operations, at least not without significant additional effort.

Objective

The aim of this module is to cover the basic security requirements to be considered when planning, purchasing, commissioning, running and decommissioning a specialised application.

Not in Scope

This module focuses on organisational and design-related aspects of information security in specialised applications. This module only describes the selection, configuration and secure operation of security functions in a general and basic manner. A detailed description of widely used standard applications is included in further modules of the layer *APP Applications*, as well as in the module *CON.4 Selection and Use of Standard Software*.

Threat Landscape

The following specific threats and vulnerabilities are of particular importance for the module *CON.5 Development and Use of Generic Applications*:

Loss of Confidentiality or Integrity in Specialised Applications

Specialised applications are typically used for processing confidential information – for example, any type of personal data or business secrets. If such data is disclosed or unintentionally changed, this may result in breaches of contract or law (including infringements of data protection law). Particularly in the case of a loss of integrity, breaches of law may occur due to process-related or procedural errors. If the information is no longer available, it will no longer be

possible to fulfil business processes or specialised tasks. The loss of confidentiality, integrity and availability may thus have a serious impact, including in the form of criminal and financial consequences or even personal injury in individual cases.

Incorrect Administration of Site and Data Access Rights

If the assignment of site and data access rights is controlled poorly, this may quickly result in serious vulnerabilities, e.g. due to unchecked growth in assigned rights. This quickly results in users being granted authorisations simply upon request, or only via unnecessarily complicated methods. On the one hand, a lack of authorisations may impede one's daily work; on the other, this may lead to authorisations being granted without need, which presents a security risk.

Unsatisfactory Contractual Arrangements with an External Service Provider

Unsatisfactory contractual arrangements with an external service provider – particularly with regard to application creation, implementation support and maintenance – may give rise to various (and even serious) security problems. If the description of tasks, performance parameters or efforts is insufficient or ambiguous, this may result in a failure to implement security safeguards due to ignorance, a lack of qualification or a lack of resources. This may have various negative consequences, such as non-compliance with regulatory requirements and obligations, a lack of compliance with laws or the duty to provide information, and a failure to accept responsibility due to lost means of control.

Software Design Errors

When planning applications, programs and protocols, it is possible to make security-related design errors. These often occur when application modules and protocols intended for a certain purpose are used in other scenarios of use. If there are other relevant security requirements (e.g. if application modules and protocols intended for separate operational environments are connected to the Internet), this may result in massive vulnerabilities.

Software Vulnerabilities

Software vulnerabilities are errors that pose security risks to the data processed with the application. These security risks arise from the fact that intended security mechanisms can be or become ineffective due to technical progress, or that security mechanisms can be bypassed in a targeted manner as a result. Furthermore, software errors may result in insufficient processing performance (performance defects) or failure of the application. Possible consequences of a failure include downtime, loss of turnover or breaches of contractual arrangements or legal requirements.

Undocumented Functions

Many applications include undocumented functions integrated by the manufacturer for development and support purposes. They are typically not known to the users. Undocumented functions can become problematic if they make it possible to bypass essential security mechanisms (e.g. for access protection). This may impair the confidentiality and integrity of the processed data.

Non-Existent or Insufficient Security Mechanisms in Applications

Security mechanisms or security functions in the application should ensure that confidentiality, integrity and availability can be guaranteed to the required extent when processing in-

formation. However, the development of an application often focuses on technical functions, time frames, or budgets, which results in important security mechanisms that are too weak and can be easily bypassed (if they are present at all).

Requirements

The specific requirements of the module CON.5 *Development and Use of Specialised Applications* are listed below. As a matter of principle, the department using the application is responsible for fulfilling these requirements. In practice, such requirements can only be fulfilled if the persons in charge of IT operations (e.g. the Head of IT) and the Chief Information Security Officer (CISO) are consulted and/or involved.

Module Owner	Process Owner
Further Roles	Data Protection Officer, IT Operation Department, Process Owner, Head of IT

Basic Requirements

For module CON.5 *Development and Use of Generic Applications*, the following requirements **MUST** be implemented as a matter of priority:

CON.5.A1 Specifying Required Security Functions of Specialised Applications [IT Operation Department]

For a specialised application, the required security functions **MUST** be considered during technical selection and the application's integration into the operational IT infrastructures and processes. Suitable security functions in the specialised application **MUST** be selected and implemented on the basis of the data processed in the application and, if applicable, a supplementary risk analysis. The security functions **MUST** be documented appropriately.

CON.5.A2 Acceptance and Approval of Specialised Applications [Head of IT, Data Protection Officer]

In order to properly transfer an application as well as in the event of essential changes, a suitable testing and approval procedure **MUST** be developed. In this respect, the following **MUST** be taken into account:

- the information domain (represented by Process Owners)
- the IT Operation Department level (represented by the Head of IT)
- the information security level (represented by the Chief Information Security Officer)
- the data protection level (represented by the Data Protection Officer)
- depending on the type and complexity of an application, additional function owners, e.g. Employee Representatives

CON.5.A3 Secure Installation of a Specialised Application [IT Operation Department]

Installation instructions covering all the required application modules (libraries), the order of installation, and the configuration of the application modules **MUST** be created. The installation instructions **SHOULD** consider the required aspects regarding the installation environment. The specialised application **MUST** be installed in accordance with the installation instructions.

The installation instructions **MUST** be updated in case of changes in the application and functional updates.

CON.5.A4 Familiarising Users with the Application

Users and administrators **MUST** be familiarised with the correct use and administration of the application, including its security functions. To this end, policies and work instructions for use and administration of the application, training, briefings, manuals and online help **SHOULD** be provided, along with user support from key users.

CON.5.A5 Secure Operation of a Specialised Application [IT Operation Department]

Authorisations for using and administering a specialised application **MUST** be assigned correctly and checked regularly for correctness. Authorisations that are no longer required **MUST** be withdrawn.

It **MUST** be ensured that logging data is evaluated regularly and legally prescribed storage times for logging data are upheld.

The manufacturer of the application **MUST** provide security-critical patches and updates on the basis of suitable contractual arrangements and install them promptly. In this context, it **MUST** be ensured that patches and updates have been tested and approved appropriately in advance.

Backups and restoration drills **MUST** be performed regularly.

Standard Requirements

For module CON.5 *Development and Use of Generic Applications*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

CON.5.A6 Comprehensive Documentation of Required Application Functions

The relevant requirements the application must meet **SHOULD** be documented. This documentation **SHOULD** be updated in case of changes to the application or related functional updates.

CON.5.A7 Drawing Up a Client Concept [Head of IT]

A client concept **SHOULD** be used to ensure that applications and data pertaining to various customers are operated separately. The client concept **SHOULD** be drawn up by the operator of the multi-client-capable application and made available to the organisations using it. The necessary client separation mechanisms **SHOULD** be implemented sufficiently by the service provider.

CON.5.A8 Appropriate Control of Application Development [Head of IT]

When developing an individual application, an appropriate control and project management model SHOULD be used. Here, the required personnel qualifications, the coverage of all relevant phases during the lifecycle of the software, an appropriate development model, risk management, and quality targets SHOULD be considered in particular.

CON.5.A9 Decommissioning Applications [Head of IT]

The decommissioning of applications SHOULD be planned. All data SHOULD be clearly designated for migration, archiving or deletion. Any data that is no longer required SHOULD be securely deleted. The decommissioning of applications, as well as the corresponding IT systems and storage media, SHOULD be documented transparently.

CON.5.A10 Contingency Planning for Applications [Head of IT]

The specialised applications SHOULD be included in contingency planning.

Requirements in Case of Increased Protection Needs

Generic suggestions for module *CON.5 Development and Use of Generic Applications* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

CON.5.A11 Appropriate and Legally Compliant Procurement [Process Owner] (CIA)

When purchasing a specialised application, the existing legal and organisational regulations SHOULD be followed. If the procurement, development or operation of an application involves service providers, the relevant security aspects SHOULD be considered in the contracts.

The organisation SHOULD have defined processes and specified contact persons to ensure consideration of the relevant framework conditions. The role of certifications in connection with the choice of a provider SHOULD be clarified.

CON.5.A12 Trusted Storage (CA)

In cases involving business-critical applications, it SHOULD be checked whether the applications require protection against outages that could affect each application's manufacturer. Here, those responsible SHOULD consider fiduciary storage at an escrow agency for any materials not included with a given application (such as documented code, design plans, keys, or passwords). In such cases, the obligations of the escrow agency regarding storage and handover (when can the stored goods be handed out, and to whom?) SHOULD be specified by contract.

CON.5.A13 Developing a Redundancy Concept for Applications [Process Owner, Head of IT] (A)

If there is a high or very high protection need regarding the availability of an application, a redundancy concept SHOULD be drawn up. This SHOULD include the following aspects:

- planning for limited IT operations and recovery in case of an emergency (contingency planning concept)

- redundancy at the application level by means of load balancing or application clusters / cloud services
- options for moving the applications to other systems

In addition, it SHOULD be ensured that the redundancy concept also includes the buildings, rooms, systems and communication links required for operation of the application. The redundancy concept SHOULD be synchronised with the contingency concept. The safeguards in the redundancy concept SHOULD be tested and exercised regularly.

Additional Information

For more information about threats and security safeguards for module *CON.5 Development and Use of Generic Applications*, see the following publications, among others:

[12207]	ISO/IEC 12207:2008: System and software engineering - Software life cycle process, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 7, February 2008
[15408]	ISO/IEC 15408-2:2008: Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 7, August 2008
[27001A14]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, especially Annex A, A.14 System acquisition, development and maintenance, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[ISFBA]	The Standard of Good Practice for Information Security: Area TS2 Cryptography, Information Security Forum (ISF), June 2018
[NIST80053F145]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, especially Appendix F-PS Page F-145, Family: System and Services acquisition, Family: System and communications protection and Family: System and information integrity, April 2013

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module *CON.5 Development and Use of Generic Applications*:

- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.18	G 0.19	G 0.22	G 0.23	G 0.26	G 0.28	G 0.29	G 0.30	G 0.31	G 0.38	G 0.39	G 0.45	G 0.46
CON.5.A1	X	X		X						X	X	X	X
CON.5.A2	X		X	X	X	X						X	
CON.5.A3				X									
CON.5.A4		X						X	X			X	X
CON.5.A5		X		X				X	X	X	X	X	X
CON.5.A6	X	X											
CON.5.A7	X	X					X						
CON.5.A8	X			X	X	X							X
CON.5.A9		X								X		X	
CON.5.A10												X	
CON.5.A11				X	X		X	X	X		X		
CON.5.A12			X									X	
CON.5.A13												X	



CON.6: Deleting and Destroying Data and Devices

Description

Introduction

In order to ensure that information does not fall into the wrong hands, standard procedures are necessary for the complete and reliable deletion and destruction of data and storage media. Sensitive information stored on analogue and digital storage media must be considered here.

If storage media are passed to third parties, sold or disposed of without being erased or only erased inadequately, this may result in unintended disclosure of information and significant. Every organisation must thus have a procedure for secure deletion and destruction.

Objective

This module describes how information in organisations can be securely deleted and destroyed and how a corresponding concept should be created.

Not in Scope

This module only includes the general process-related, technical and organisational requirements for deletion and destruction. Individual modules in the layers CON (*Concepts and Approaches*), ISMS (*Security Management*), ORP (*Organisation and Personnel*), OPS (*Operation*), DER (*Detection and Reaction*), IND (*Industrial IT*), APP (*Applications*), SYS (*IT Systems*), NET (*Networks and Communication*) and INF (*Infrastructure*) may define supplementary and specific requirements for deletion and destruction. Above all, the modules CON.3 *Backup Concept*, OPS 1.2.2 *Archiving* and OPS.1.2.3 *Exchange of Information and Storage Media* should also be considered, as these topics are directly linked to deletion and destruction.

Threat Landscape

For module CON.6 *Deleting and Destroying Data and Devices*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficiently Documented Regulations for Deletion and Destruction

If there are no documented processes and procedures for deleting and destroying information and storage media (or they are not used correctly), confidential information cannot be destroyed securely and may thus fall into the wrong hands. This risk is particularly high with storage media and IT systems designated for disposal because inappropriate regulations may result

in information remaining on said media. Such data can be read or stolen by unauthorised third parties. If this includes information crucial to an organisation's existence, it may threaten the entire organisation.

Loss of Confidentiality Due to Residual Information on Storage Media

When data is communicated electronically or storage media are transferred, it is not unusual for information that should not be passed on to leave the organisation.

With most file systems, files deleted by the user are not fully destroyed. Only the references to the file are deleted from the administration information of the file system and the blocks that belong to the file are marked as free. However, the actual content of the blocks on the storage medium is retained and can be reconstructed with appropriate tools. This can enable attackers to get access to the file, such as when storage media are handed over to third parties or disposed of in an inappropriate manner. Confidential information may thus leak outwards.

Unstructured Data Organisation

Inadequate specifications and a lack of employee training can lead to information being stored in a confusing way on storage media. This may make it impossible to delete information completely because there is no longer a person responsible who knows what the stored files actually include. Attackers may also access information covertly if there are many copies of a file and such copies are present in various directories with different protection functions. Copies are often not only stored in various directories of a storage medium. It is much more critical when several copies are stored on different storage media and the place and time of the storage of certain content are no longer obvious. This problem gets even worse if the storage media are neither purchased centrally nor controlled. Unstructured data organisation threatens not only availability (working with data), but integrity and confidentiality, as well.

Loss of Confidentiality Due to Swap Files and Temporary Files

Swap files or swap partitions can include confidential data such as passwords or cryptographic keys. Swap files and the information they contain, however, are not protected as they can be read by removing the hard disk and installing it in another IT system (for example).

The live operation of many applications also produces files not required for production operation (e.g. browser histories). Such files can also include security-relevant information. If swap files or temporary files are not securely deleted, then sensitive information, passwords and keys can be misused by unauthorised parties to get access to further IT systems and data, obtain competitive edges on the market, or spy on the behaviour of users in a targeted manner.

Inadequate Disposal of Storage Media and Documents

If storage media or documents are not disposed of properly, it is possible under certain circumstances to extract information from them that should not fall into the hands of third parties. For example, attackers may steal storage media from inappropriately secured disposal facilities. If commissioned disposal service providers are not sufficiently supervised, confidentiality cannot be ensured as required.

Requirements

The specific requirements of module CON.6 *Deleting and Destroying Data and Devices* are listed below. As a matter of principle, the CISO is responsible for fulfilling the requirements. The

Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	IT Operation Department, Data Protection Officer, Head of Building Services, Head of Organisation, Employee, Procurement Department, Process Owner, Head of IT

Basic Requirements

For module CON.6 *Deleting and Destroying Data and Devices*, the following requirements **MUST** be implemented as a matter of priority:

CON.6.A1 Regulations Governing the Procedure for Deleting or Destroying Information [Head of IT, Head of Organisation]

The organisation **MUST** regulate the deletion and destruction of information. In this regard, the information and resources that can be deleted, as well as the prerequisites for this, **MUST** be specified depending on the organisational unit. Furthermore, it **MUST** be specified where disposal and destruction facilities should be placed.

In addition, the persons responsible for deleting and destroying information and resources and the interfaces between the organisational units **MUST** already be specified during the planning phase. Furthermore, the internal flow of information, as well as the flow of information between the responsible persons of the organisation and possible outsourcing service providers, **MUST** be regulated.

CON.6.A2 Correct Disposal of Sensitive Resources and Information [Employee, Head of Building Services, Head of IT]

All sensitive resources and information **MUST** be disposed of securely. To this end, secured and suitable disposal facilities **MUST** be available on the property of the organisation. In this regard, it **MUST** be considered that information and resources may be collected first and only disposed of later on. A central collection point of this kind **MUST** be protected against unauthorised access.

If external service providers are commissioned, the disposal process **MUST** be sufficiently secure and transparent. The companies contracted for disposal **SHOULD** be checked at regular intervals as to whether the disposal process still corresponds to the target state.

Standard Requirements

For module CON.6 *Deleting and Destroying Data and Devices*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

CON.6.A3 Deleting Storage Media Before and After Exchange [Process Owner]

Before forwarding or reusing storage media, any data on them SHOULD be securely deleted. Employees SHOULD have access to appropriate methods of doing so (see CON.6.A4 *Selecting Suitable Methods for Deleting or Destroying Storage Media*).

CON.6.A4 Selecting Suitable Methods for Deleting or Destroying Storage Media [Head of IT, Head of Organisation]

Appropriate methods SHOULD be selected for deletion and destruction. For example, there SHOULD be appropriate devices and tools for the various types of storage media that the responsible employee can use for deleting and destroying the stored information. It SHOULD be checked regularly that the selected methods still correspond to the state of the art and are sufficiently secure for the organisation. The selected procedures SHOULD be known to all employees.

CON.6.A5 Controlled Decommissioning of IT Systems and Storage Media [IT Operation Department, Employee, Process Owner, Head of IT]

It SHOULD be regulated and documented how IT systems and storage media are to be decommissioned. In this regard, it SHOULD be ensured that all information stored on IT systems or storage media are securely deleted before disposal. During disposal, all IT systems containing permanent memory elements SHOULD be considered in addition to “traditional” IT systems.

CON.6.A6 Employee Instruction on Methods of Deleting or Destroying Information [Head of IT]

All employees SHOULD be instructed on the methods and procedures for deleting and destroying information. In this regard, the requirements of module ORP.3 *Awareness and Training* SHOULD be fulfilled.

CON.6.A7 Removal of Residual Information [IT Operation Department, Employee]

If storage media and files are to be forwarded, it SHOULD be ensured that they do not contain residual information. A corresponding process SHOULD be established and documented in the organisation. The employees SHOULD be informed of the risks of residual and additional information in files so that they can sufficiently implement this process. It SHOULD be checked at random whether the residual information included in files is actually deleted.

CON.6.A8 Policy for Deleting and Destroying Information [Employee, Head of IT, Data Protection Officer]

The regulations of the organisation regarding deletion and destruction SHOULD be documented in a policy. The policy SHOULD be known to all relevant persons in charge and employees of the organisation and SHOULD represent the basis for their actions and work. Regarding its content, the policy SHOULD include all employed storage media, applications, IT systems and other resources and information that are subject to deletion and destruction. It SHOULD be checked regularly and at random whether the employees are complying with the policy. The policy SHOULD be updated at regular intervals.

Requirements in Case of Increased Protection Needs

Generic suggestions for module CON.6 *Deleting and Destroying Data and Devices* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security

objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

CON.6.A9 Selecting Suitable Methods for Deleting or Destroying Storage Media with Increased Protection Needs [Head of IT, Head of Organisation] (CIA)

Methods that are appropriate for the increased protection needs of information and resources SHOULD be selected for deletion and destruction.

CON.6.A10 Purchasing Suitable Devices for Deleting or Destroying Data [Head of IT, Procurement Department, Head of Organisation] (CIA)

Before purchasing devices for deleting or destroying data, a requirements document for comparing tools available on the market SHOULD be created.

CON.6.A11 Destruction of Storage Media by External Service Providers [Head of Organisation, Data Protection Officer] (CIA)

All storage media SHOULD be stored on the property of the organisation in a secure manner protected against unauthorised access until they are picked up by the external service provider. The removal also SHOULD be secured in accordance with the protection needs. The organisation SHOULD have the disposal process checked by trained personnel at regular intervals.

Furthermore, the general requirements for service providers and their employees SHOULD be implemented as described in OPS.2.1 *Outsourcing for Customers*.

Additional Information

For more information about threats and security safeguards for module CON.6 *Deleting and Destroying Data and Devices*, see the following publications, among others:

[27001A8.3]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, especially Annex A, A.8.3 Media handling, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[DIN663991]	DIN 66399-1:2012-10 Office machines - Destruction of data carriers - Part 1: Principles and definitions, October 2012
[DIN663992]	DIN 66399-2:2012-10 Office machines - Destruction of data carriers - Part 2: Requirements for equipment for destruction of data carriers, October 2012
[DIN663993]	DIN SPEC 66399-3:2013-02 - Office machines - Destruction of data carriers - Part 3: Process for destruction of data carriers, February 2013
[SP80088]	Guidelines for Media Sanitization: NIST Special Publication 800-88, Revision 1, December 2014, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module CON.6 *Deleting and Destroying Data and Devices*:

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.44 Unauthorised Entry to Premises

Elementary Threats Requirements	G 0.18	G 0.19	G 0.31	G 0.44
CON.6.A1	X	X		
CON.6.A2		X		X
CON.6.A3		X	X	
CON.6.A4		X		
CON.6.A5		X		
CON.6.A6		X	X	
CON.6.A7		X	X	
CON.6.A8	X	X	X	
CON.6.A9		X		
CON.6.A10		X	X	
CON.6.A11		X		X



CON.7: Information Security on Trips Abroad

Description

Introduction

The importance of necessary work-related travelling has increased steadily in recent years as a result of globalisation and the resulting increased international networking of public authorities and companies. To be able to continue working outside the normal work environment, it has become inevitable that people travel with both hard-copy documents and information technology – laptops, smartphones, tablets, removable hard drives or USB pen drives, for example. For business trips, in particular when travelling abroad, a multitude of threats and risks need to be taken into account for information security that do not exist during normal business operations.

Each trip is fundamentally different since the threat landscape is always changing, including in relation to the protection of business-critical information, depending on parameters such as the purpose of the trip (e.g. a business meeting, conference, congress, or seminar), the duration of the trip and the destination.

Due to the constantly changing destinations, specific circumstances and regulatory and legal requirements, it is not always easy to protect operational information. Legal and regulatory requirements, for example, may affect border control checks, and thus preservation of data confidentiality. This demonstrates that there are individual information security requirements depending on the type and duration of the trip, as well as the destination. Political, societal, religious, geographical, climatic, legal and regulatory particularities play a significant role here.

Objective

The objective of this module is to protect all information which is taken on trips abroad both in electronic and physical form with regard to confidentiality, integrity and availability. The confidential information which all travelling employees take with them in the form of knowledge is also the subject of this module. As a result, the establishment of appropriate regulations and measures for dealing with sensitive information and data on trips abroad while factoring in other relevant framework conditions (such as IT, data protection, and laws) is essential.

As a result, this module indicates scenario-specific threats and requirements which relate directly to the secure use of information technology, information and the devices used to process it on trips abroad.

This module is designed to be used by the responsible parties in an organisation as a guide to establishing appropriate security measures in the context of information security on trips abroad. It indicates the fundamental principles which should be taken into account in this regard. Many of the threats specified are also relevant for domestic travel, or in general when handling information in foreign environments or environments which are not under the organisation's control.

Not in Scope

The module inherently includes the requirements which contribute to the appropriate protection of information on trips abroad. Here, the protection of the confidentiality and integrity of sensitive information has the same importance on trips as at the organisation's headquarters.

Threats and requirements relating to the local information domain are not taken into consideration here.

Since the process-related, technical and organisational requirements which are specific to business-related work while travelling are taken into account in particular in the module CON.7 *Information Security on Trips Abroad*, the requirements in the layers NET *Networks and Communication*, SYS *IT Systems* and APP *Applications* are not considered. All the necessary modules, especially SYS.2.1 *General Client*, NET.3.3 *VPN* and SYS 3.2.2 *Mobile Device Management (MDM)*, must be taken into consideration separately.

In addition, the requirements of the overlapping modules INF.9 *Mobile Workplace* and OPS.1.2.4 *Teleworking* should be considered and implemented.

Within this module, there are also overlaps with other modules and topic areas which are not taken into consideration here:

- fulfilment of data protection requirements
- preventive measures for the protection of information (including technical demands which are made on portable IT systems, e.g. emission and eavesdropping protection)
- personal security

Threat Landscape

The specific threats and vulnerabilities in the field of information security which are of particular importance on trips abroad are described below.

For some threats, the threat level is particularly elevated due to the nature of such scenarios. This results, for example, from communication over public networks which are not under the organisation's control. This means that risks against which the organisation has perhaps already secured itself become relevant once again.

In addition, the probability of a risk occurring while travelling abroad is usually significantly higher than for domestic travel depending on the selected destination country.

Eavesdropping and Spying on Information/Industrial Espionage

Espionage refers to attacks that aim to collect, evaluate and process information about organisations, people, products or other target objects. Particularly when travelling abroad, there are unknown sources of risk over which the information security management of the organisation in question is unable to exercise any influence. As a general rule, foreign spaces and IT environments present many risks stemming from targeted eavesdropping on in-person discussions, communication lines, phone conversations and data transmissions. Particularly when abroad, this can be problematic and difficult to assess for travellers with regard to the legal options available in such cases.

This can concern both public spaces and rooms and circumstances in other organisations, as well as the organisation's own representatives' offices abroad. Devices such as mobile phones, for example, can also be used to record or listen to conversations unnoticed. In addition, many IT systems come equipped with a microphone and camera, which can be accessed and then used.

Furthermore, there may be restrictions when entering or leaving certain countries which override or contradict the regulatory provisions in the country of origin and the organisation's requirements. One example involves the possibility that access to data stored on laptops and other portable IT systems can be requested upon entry to other countries, such as the USA. Confidential and personal data can, to some extent, not only be viewed, but even copied and saved in the process. Since this information may include strategic papers or strictly confidential drafts from a company or a public authority, for example, it is always necessary to reckon with the potential misuse of such information in this context (industrial espionage).

Furthermore, signals cannot be shielded physically against unauthorised eavesdropping or recording during transmission. As a result, access points/hotspots and similar interfaces could be attacked or eavesdropped on, and information could be gathered through them. This includes location information or MAC addresses, for example, but also data packets which are transmitted unencrypted and information such as metadata (such as recipient and sender data, addresses or telephone numbers).

When travelling abroad, there are risks beyond information being intercepted in a technically complex manner. Sensitive data can often simply be spied on using optical, acoustic or electronic methods since the usual standards of security regulations in relation to information security cannot be expected in many cases. For instance, this affects the general security level which prevails in other countries and the local circumstances which a traveller is obliged to deal with.

Consider the unencrypted transmission of user IDs and/or passwords, for example, as well as threats such as unlocked or easily readable screens via which an attacker can access information.

Disclosure and Misuse of Sensitive Information (Electronic and Physical)

When exchanging information, whether by sending or handing over storage media or sharing information in person or over the phone, it is often the case that other sensitive information is conveyed unintentionally along with the desired information. This must also be considered when travelling abroad. Here, communicating and exchanging information is, to some extent, made even more difficult by technically insecure circumstances. In addition, business travellers may leave confidential documents in both physical and electronic forms lying visible in public places or in hotel rooms due to carelessness.

Communicating with unknown IT systems and networks always poses a potential threat to travellers' own end devices. For example, confidential information which is not intended to be disclosed can be copied in this way.

Meanwhile, foreign storage media can also contain malware. Here, there is the risk that important data could be stolen, manipulated, encrypted or erased. At the same time, the integrity and availability of IT systems may also be impaired. This aspect is promoted by the fact that data exchanges abroad often occur via insecure media. However, employees are not always aware of this important aspect.

Unnoticed Access to Mobile End Devices

Portable end devices such as laptops, smartphones, tablets or PDAs are generally designed to make it easy to exchange data with other IT systems. This may be performed using a connecting cable or wirelessly (via WLAN, Bluetooth, or GSM, for example). Where open access to IT systems is possible when travelling abroad, attackers are consequently able to request, change or obtain information unnoticed from mobile end devices under some circumstances. Subsequent checks or proof of such events are not always possible because the access attempts are often not subject to corresponding logging.

Use of False Identities

Communication while travelling involves an increased risk of attackers seeking to simulate a false identity both in person and electronically, or to assume an authorised identity (by technical means such as masquerades, spoofing methods, hijacking, or man-in-the-middle attacks). Here, users can be deceived regarding their communication partner's identity such that they disclose sensitive information. A false digital identity can be obtained by spying on a user ID and password, manipulating the sender field of a message or manipulating an address in the network, for example.

An employee does not always know foreign business partners personally. As a result, an employee may believe the first person who presents themselves with the right name and background knowledge and pass on valuable information to them.

Since the security requirements for confidentiality and integrity can never be fully guaranteed in buildings and spaces outside the organisation (particularly abroad), there is also always a residual risk that even things which appear self-evident can be manipulated. These include the phone numbers displayed on a telephone or the sender identification on fax machines, which make it possible to simulate a false identity and obtain information.

Lack of Security Awareness and Carelessness in Handling Information

While a number of organisational regulations and technical security procedures for portable IT systems and mobile storage media are often in place in organisations, they are then undermined through careless handling of the specifications and the technology. Mobile storage media left unattended in a meeting room during breaks or even in a train compartment are a common sight, for example.

In addition, gifts in the form of storage media (e.g. USB pen drives) are sometimes accepted by employees and indiscriminately connected to their own laptops. Here, there is the risk that the laptop will be infected with malware and sensitive data will be stolen, manipulated or encrypted and thus temporarily (see 2.7 Coercion, Extortion, Hijacking and Corruption) made unusable.

On public transport or even during business meals, people can often be observed conducting open conversations about business-critical information. This can then easily be overheard by outsiders and potentially used to seriously disadvantage the employee or their organisation.

Violation of Local Laws or Regulations

When travelling abroad, differing laws and regulations and additional provisions in the destination country should be taken into account in particular, as they can differ significantly from one's national legal situation. Relevant laws and regulations (e.g. concerning data protection, information requirements, liability, or information access for third parties) in the destination country are often not known to or incorrectly assessed by travellers. As a result, a multitude of laws can be violated not just abroad, but also at home – for example, if personal data concerning national customers is transmitted without protection over public networks while on a business trip abroad.

Coercion, Extortion, Hijacking and Corruption

The security of information, and also of the travellers themselves, can be compromised through coercion and extortion (and in such contexts with hijacking, as well) while travelling abroad. When abroad, there are often other security risks resulting from political and social circumstances. Employees can become victims when they are threatened with violence in order to force them to disclose sensitive information. In the process, they are forced to circumvent or disregard security policies and measures. The focus here is often on high-level managers or employees who enjoy a particular position of trust.

Attackers predominantly aim to steal or manipulate sensitive information in order to interfere with the course of business processes or to make themselves and others rich. The attackers are often driven by political, ideological and financial goals.

Alongside the threat of violence, there is also the possibility that travellers may specifically be offered money or other benefits (bribery) in order to persuade them to surrender confidential information to unauthorised persons or to commit breaches of security (corruption). In general, coercion, extortion (as well as hijacking in this connection) and corruption are used to disrupt or entirely circumvent the implementation of the applicable regulations in information security.

Information or Products from an Unreliable Source/Fraud

While working abroad, travellers can deliberately be sent false (misleading) information in order to deceive them. As a result of this deception, incorrect statements may be incorporated into business-critical reports. Amongst other things, this may lead to business-relevant information being based on false data, calculations providing incorrect results and wrong decisions being taken as a result.

Degradation of IT Due to Different Operational Environments

When travelling, information technology is used in a very wide range of environments and is therefore subject to many threats. These threats include, for example, damaging environmental conditions such as excessively high or low temperatures, dust, and moisture. Other problems resulting from the portability of devices include damage sustained during transport.

In addition, operational IT processes which often do not extend to environments abroad (such as patch management, change management and access management) result in vulnerabilities which can quickly be exploited, particularly in unsecured IT networks.

Theft or Loss of Devices, Storage Media and Documents

Particularly on trips abroad, it should be expected that mobile end devices can easily be lost or stolen. The smaller and more popular these devices are, the higher the risk of them being stolen becomes. Alongside the purely material damage stemming from the immediate loss of the mobile device, the publication of sensitive data (e.g. e-mails, notes from meetings, addresses or other documents) can result in additional (financial and/or reputational) damage.

Requirements

The specific requirements of module *CON.7 Information Security on Trips Abroad* are listed below. As a matter of principle, the Chief Information Security Officer is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements.

Furthermore, the CISO is responsible for ensuring that all requirements are regularly verified according to the security concept defined.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Human Resources Department, Data Protection Officer, BCM Officer, IT Operation Department, User, Process Owner

Basic Requirements

For module *CON.7 Information Security on Trips Abroad*, the following requirements **MUST** be implemented as a matter of priority:

CON.7.A1 Security Policy for Information Security on Trips Abroad

All aspects which are relevant to information security in connection with working abroad **MUST** be considered and regulated. Requirements for security measures which are taken in this connection **MUST** be documented in a security policy for information security on trips abroad. The regulations and the security policy for information security on trips abroad (or an information sheet on information security on trips abroad in which the security measures to be taken are set out) **MUST** be handed out to employees who work in multiple countries.

In addition, a security concept for handling portable IT systems on trips abroad in which all security requirements and measures are described in adequate detail **MUST** be established and regularly reviewed.

CON.7.A2 Raising Employee Awareness of the Security Policy for Information Security on Trips Abroad [Data Protection Officer, IT Operation Department]

Users **MUST** be trained in and made aware of the responsible handling of information technology and portable IT systems on trips abroad. In particular, they **MUST** be made aware of the risks which arise from inappropriate handling of information, improper destruction of data

and storage media, malware and non-compliant data exchange, and the limits of the security measures used must also be demonstrated to them. They **MUST** be empowered and encouraged to seek expert advice in the event of inconsistencies and to prevent loss or theft. In addition, the legal requirements for individual destinations in relation to travel security **SHOULD** be emphasised to employees. Here, the responsibility for obtaining information about legal requirements in the context of information security (e.g. data protection and the German IT Security Act) and providing it to employees lies with the Chief Information Security Officer.

CON.7.A3 Identification of Country-Specific Regulations, Travel Conditions and Environmental Conditions [Human Resource Department]

Before the beginning of a trip, the person responsible for information security management or the Human Resource Department **MUST** review the applicable regulations for the country in question and communicate them to the relevant employees.

The organisation **MUST** establish, implement and communicate suitable regulations and safeguards which allow for appropriate protection of internal data depending on the individual travel and environmental conditions.

In addition, before the beginning of a trip, employees **MUST** familiarise themselves with the climatic conditions in the destination country and clarify which protective measures they require for themselves (e.g. vaccinations) and the information technology they plan to take along.

CON.7.A4 Use of Privacy Films [User]

Particularly when abroad, users **MUST** take care to ensure that no sensitive information can be spied on when working on a laptop, for example. To this end, appropriate privacy screens which cover the entire screen of the respective device (laptops, tablets or smartphones) and thwart information espionage **MUST** be used on all mobile IT systems.

CON.7.A5 Use of Screen/Code Locking [User]

The use of screen/code locking prevents third parties from being able to access data on mobile end devices such as laptops or mobile phones. An appropriate locking option **MUST** be used. For this, the user **MUST** use an appropriate code or a secure device password. Screen locking **MUST** automatically activate after a short period of inactivity.

CON.7.A6 Prompt Reporting of a Loss [User, BCM Officer]

Employees **MUST** report any loss or theft of information, IT systems or storage media to their organisation immediately. To this end, there **MUST** be clear reporting channels and contact persons within the organisation. The organisation **MUST** evaluate the possible impacts of the loss and take appropriate countermeasures.

CON.7.A7 Secure Remote Access [IT Operation Department, User]

In order to allow secure remote access to the organisation's network for employees on trips abroad, secure remote access (e.g. via VPN) **MUST** be set up by the IT Operation Department in advance. The VPN access **MUST** be cryptographically secured. In addition, users **MUST** have appropriately secure access data in order to successfully authenticate themselves on end devices and the network. Employees **MUST** use the secure remote access for all communications which are possible in this context. Care **MUST** be taken to ensure that only authorised persons can access the IT systems which have remote access. To the greatest extent possible, mobile IT systems **MUST** be protected against direct access to the internet by a restrictively configured personal firewall.

CON.7.A8 Secure Use of Public WLANs [User]

Whether or not mobile IT systems will be allowed direct access to the internet **MUST** always be specified.

Access to the organisation's network via publicly accessible WLANs **MUST** be granted via a virtual private network (VPN) or comparable security mechanisms (see CON.7.A7 *Secure Remote Access*). The secure use of WLANs is described in module NET.2.2 *WLAN Usage*. The use of WLAN hotspots **MUST** also be secured as described in module INF.9 *Mobile Workplace*.

CON.7.A9 Secure Handling of Mobile Storage Media [User]

Before mobile storage media are used, they **MUST** be checked for malware. Before passing on mobile storage media, users **MUST** ensure that they do not contain any sensitive information. After use, a storage medium **MUST** be securely erased, particularly if it is being passed on to someone else. To this end, the storage medium **MUST** be overwritten using a sufficiently secure method determined in an organisation.

CON.7.A10 Encryption of Portable IT Systems and Storage Media [User, IT Operation Department]

In order to ensure that sensitive information cannot be viewed by unauthorised third parties, employees **MUST** ensure before the beginning of a trip that all such information is secured in accordance with the internal guidelines. To this end, mobile storage media and clients **SHOULD** be encrypted before the beginning of a trip. The cryptographic keys **MUST** be stored separately from the encrypted device. When encrypting the data, the statutory regulations of the destination country **SHOULD** be observed. This particularly applies to local provisions on the disclosure of passwords and the encryption of data.

CON.7.A11 Use of Anti-Theft Devices [User]

For the protection of mobile IT systems outside the organisation, anti-theft devices **SHOULD** be used, particularly in places dominated by higher public traffic or where the fluctuation of users is very high. The procurement and usage criteria for anti-theft devices **SHOULD** be adapted to the organisation's processes and documented.

CON.7.A12 Secure Destruction of Sensitive Materials and Documents [User]

Particularly abroad, it is not always possible to dispose of documents and other sensitive storage media securely. The organisation **MUST** present employees with options for appropriately destroying business-critical documents. The employees **MUST** comply with these options and **MUST NOT** dispose of the organisation's internal documents publicly. If this is not possible locally or it involves dealing with documents or storage media containing particularly sensitive information, these items **MUST** be kept until the employee's return and then appropriately destroyed.

Standard Requirements

For module CON.7 *Information Security on Trips Abroad*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

CON.7.A13 Transportation of Data and Storage Media [IT Operation Department, User]

Before departing on a trip, employees **SHOULD** check which data on the IT systems they plan to take along (such as laptops, tablets or smartphones) will not be absolutely required during

the trip. If it is not necessary to retain this data on the devices, it SHOULD be physically deleted (see CON.7.A9 *Secure Handling of Mobile Storage Media*). However, should the need arise to take sensitive data on trips, this SHOULD only be done in an encrypted form.

In addition, the mobile storage media that may be taken on trips abroad and the corresponding security measures that should be taken into account (e.g. protection against malware, encryption of business-critical data, storage of mobile storage media) SHOULD be established in writing. The employees SHOULD know and observe these regulations before departing on the trip (see, among others, CON.7.A12 *Encryption of Portable IT Systems and Storage Media*).

These security-related requirements vary depending on the protection needs of the data to be handled abroad and the data to be accessed.

CON.7.A14 Cryptographically Secured E-Mail Communication [User, IT Operation Department]

Employees SHOULD secure e-mail-based communications cryptographically in accordance with the organisation's internal provisions.

For communication via e-mail services (e.g. webmail), the organisation SHOULD clarify in advance what security mechanisms are implemented by the provider and whether they satisfy its internal security requirements. These include, for example, secure operation of the server, the establishment of an encrypted connection and the duration of data storage. E-mails SHOULD also be suitably encrypted or digitally signed. Public IT systems, such as those in hotels or internet cafés, SHOULD not be used for accessing e-mails.

Requirements in Case of Increased Protection Needs

Generic suggestions for module CON.7 *Information Security on Trips Abroad* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

CON.7.A15 Emission Security for Portable IT Systems [IT Operation Department] (C)

Before the beginning of the trip, the protection needs for the particular information which will be handled on the employee's mobile storage media or client while abroad SHOULD be determined. Emissions containing information, or even compromising emissions from these storage media and clients, can be received or intercepted by others such that information can be reconstructed and its confidentiality called into question. Here, the organisation SHOULD check whether there is a related protection need for confidential information and use appropriate low-emission and secure storage media and clients.

CON.7.A16 Protecting Integrity Using Checksums or Digital Signatures (I)

Checksums SHOULD be used in the context of data transmission and backups in order to be able to check the integrity of the data. Better yet, digital signatures SHOULD be used in order to safeguard the integrity of sensitive information.

CON.7.A17 Use of Dedicated Travel Hardware [IT Operation Department] (CIA)

In order to prevent the unauthorised outflow of the organisation's sensitive information on trips abroad (e.g. upon entry or departure), pre-configured travel hardware SHOULD be

provided to the employees. On the basis of the minimum principle, this travel hardware SHOULD only provide the functions and information which are absolutely necessary to conduct the business activities.

CON.7.A18 Restricted Authorisations on Trips Abroad [Process Owner, IT Operation Department] (CI)

Before departing on a trip, the Process Owner for security management in the organisation SHOULD check what authorisations employees really need in order to pursue their day-to-day business while abroad. To this end, the possibility of withdrawing access rights for the duration of the user's trip in order to prevent unauthorised access SHOULD be considered.

Additional Information

For more information about threats and security safeguards for module CON.7 *Information Security on Trips Abroad*, see the following publications, among others:

[IWS]	Initiative Wirtschaftsschutz [Economic Protection Initiative]: https://www.wirtschaftsschutz.info , last accessed on 28.08.2018
-------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module CON.7 *Information Security on Trips Abroad*:

- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.17 Loss of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.35 Coercion, Blackmail or Corruption
- G 0.36 Identity Theft
- G 0.39 Malware

G 0.42 Social Engineering

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.1 4	G 0.1 5	G 0.1 6	G 0.1 7	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 9	G 0.3 0	G 0.3 1	G 0.3 5	G 0.3 6	G 0.3 9	G 0.4 2	G 0.4 5	G 0.4 6
CON.7.A1	X		X	X	X	X		X	X	X						
CON.7.A2	X				X		X	X		X				X		
CON.7.A3				X	X	X		X	X						X	X
CON.7.A4			X			X			X				X			
CON.7.A5			X			X		X	X				X			
CON.7.A6						X			X							
CON.7.A7	X	X					X		X							
CON.7.A8		X			X	X	X	X		X						
CON.7.A9			X			X	X									
CON.7.A10					X	X		X				X				X
CON.7.A11			X	X					X	X					X	
CON.7.A12			X		X	X		X		X						
CON.7.A13			X	X	X	X			X		X				X	X
CON.7.A14	X	X				X	X	X				X				X
CON.7.A15									X			X				
CON.7.A16							X			X					X	X
CON.7.A17	X				X				X		X				X	
CON.7.A18					X					X						



OPS.1.1.2: Proper IT Administration

Description

Introduction

The ongoing administration of IT systems and components is fundamental for IT operations. System administrators configure IT systems and applications, monitor operations and react by taking measures to maintain the function and capability of the systems, or they adapt the systems to changing needs. They also fulfil a number of tasks for security in doing so: besides ensuring that systems remain available, they implement security safeguards and check that these are effective. To this end, they have comprehensive authorisations, which is why it is very important for the security of an information domain that system administration itself be protected against unauthorised access.

Objective

The objective of this module is to show how the security requirements of IT applications, systems and networks can be met by means of proper IT administration.

By implementing this module, the organisation can ensure that the activities required for the security of the information domain are performed properly and systematically in system administration. At the same time, the organisation can react to the special threats that inevitably result from handling administration privileges and being able to access sensitive areas of the organisation.

Not in Scope

This module describes general security requirements regarding proper IT administration. In doing so, it considers ongoing administrative activities performed by dedicated personnel at the locations of the organisation. The module must be differentiated from remote administration of IT systems using external interfaces, as well as from remote maintenance of devices and components performed by the respective manufacturers or suppliers, which is considered in module OPS.2.4 *Remote Maintenance*.

The objects of the present module include comprehensive requirements regarding the administration process itself. Specific requirements regarding the process of managing individual IT systems and components are addressed in module OPS.1.1.7 *System Management*. There, corresponding requirements as to how systems are to be installed and commissioned and how changes and maintenance work is to be performed (or systems decommissioned) can be found.

The additional modules in OPS.1.1 *Core IT Operation* describe aspects of IT operations that are relevant in addition to the present module. As a consequence, they should also be considered and modelled as a complement to this module.

The proper administration of users and rights is of particular relevance to the security of an organisation. As a consequence, this subject is also addressed in a separate module (see ORP.4 *Identity and Access Management*).

The requirements described in the present module must also be applied if administrative tasks are performed by third parties. Particular requirements for such cases are also described in the modules OPS.2.1 *Outsourcing for Customers* and OPS.3.1 *Outsourcing for Service Providers*.

Furthermore, the module on proper IT administration refers to normal operations. In exceptional situations, particularly in the event of a possible IT attack and compromised systems, deviating requirements must be observed that are described in the corresponding modules from the field of DER.2 *Security Incident Management*.

Threat Landscape

For module OPS.1.1.2 *Proper IT Administration*, the following specific threats and vulnerabilities are of particular importance:

Failures Caused by Unspecified Responsibilities

If IT organisations have not unambiguously specified the administrative responsibilities (e.g. in the fields of planning, installation, documentation, patch management and monitoring) or the employees involved are not familiar with or do not understand the rules, this may result in security-relevant tasks from these fields not being performed, or being performed in a non-systematic manner. Typical examples include an unclear delimitation of the responsibilities between IT and telecommunications technology, between office IT and production systems, or between application and platform operations.

Shortage of Personnel with Core Competencies

Administrators may also be unexpectedly absent for extended periods of time. If they do not have trained substitutes, the continued orderly operation of the systems and applications they support will not be guaranteed. Administrators sometimes build up highly extensive and detailed knowledge of the systems and applications they support. This includes not only the products and solutions used, but particularities of the operational environment and specific configurations, as well. Based on their knowledge, they are capable of quickly identifying error situations and implementing requirements more easily, which often results in the administration being performed by a single person, especially for complex systems. If this person is absent, the knowledge is no longer available to the organisation.

Misuse of Administrative Authorisations

Administrative authorisations allow for comprehensive access to documents, communication contents and databases. Administrators may use these comprehensive authorisations in order to not only perform the tasks assigned to them, but also for their own purposes (or for third parties). This means they might view personnel documents or have access to colleagues' communication threads. Furthermore, third parties may also influence administrators by applying

pressure or using other incentives in order to access data or systems improperly with their help.

Facilitating Attacks

The privileged system access granted to administrators is frequently the focus of attackers. If administrative tasks are not performed properly, attacks on the information domain might be significantly easier as a consequence. Negligence may cause errors in configuration, lead to specified protective safeguards not being implemented sufficiently (if at all) or result in failures to follow up on suspicious events. The reasons for this include a lack of security awareness, high time pressure or a lack of processes and approaches, for example. This may result in vulnerabilities that may be exploited by attackers.

Operational Disruptions

Administrative activities have a direct influence on the operation of IT systems and applications. For example, active user sessions may be interrupted when IT systems are restarted, or authorised access may be prevented when firewall rules are being adapted. If such processes are performed without taking into account the possible effects on the users or coordinating the processes with said users, operations may be disrupted significantly.

Lack of Investigation Options for Incidents

Shortcomings regarding the documentation of IT operations or missing records may make it impossible to investigate or clear up IT security incidents. Since it is often not easy to identify (for example) how an attack occurred, what the extent of the attack was or how the manipulations were performed in the context of security incidents, such aspects must first be determined within the framework of appropriate investigations. However, this assumes that the target condition of systems prior to the security incident has been documented and can be checked, for example, or that proper changes to the systems can be differentiated from unauthorised changes based on appropriate documents. If the corresponding information is not available, incidents may only be investigated with some degree of difficulty, or not at all. In such cases, it is not possible to provide any legally valid evidence against the attackers.

Requirements

The specific requirements of module OPS.1.1.2 *Proper IT Administration* are listed below. As a matter of principle, the Head of IT is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are fulfilled and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of IT
Further Roles	Chief Information Security Officer (CISO), Head of Personnel, IT Operation Department

Basic Requirements

For module OPS.1.1.2 *Proper IT Administration*, the following requirements **MUST** be implemented as a matter of priority:

OPS.1.1.2.A1 Selection of Personnel for Administrative Tasks [Head of Personnel]

If employees are to assume administrative tasks within the IT environment, they **MUST** comply with the following criteria in consideration of the security requirements of the systems and applications they will support:

- The employees **MUST** have the necessary technical qualifications to properly handle the tasks they are assigned. They **MUST** have sufficient knowledge regarding the IT systems, applications and platforms supported in each case. The employees **MUST** have a solid command of the language used for documentation within the organisation and sufficient knowledge of the English language in order to understand typical IT documentation.
- The employees **MUST** be capable of performing the tasks they are assigned in a reliable and careful manner.
- There **MUST** be separation between administrative and supervising roles (e.g. auditing).

The administrators and their deputies **MUST** have sufficient time to carry out their tasks with due diligence. All administrators and their deputies **MUST** have sufficient opportunities for further education.

These requirements **MUST** also be met if third parties are assigned administrative tasks.

OPS.1.1.2.A2 Stand-In Arrangements and Contingency Planning

Stand-in arrangements **MUST** be made for all administrative tasks and responsibilities.

It **MUST** be ensured that only appointed deputies may access the IT systems to be supported. In order to be able to access systems and applications even during emergencies, corresponding emergency users with administration rights **SHOULD** be created.

OPS.1.1.2.A3 Controlled Hiring of IT Administrators [Head of Personnel]

If employees assume administrative tasks within the IT environment, they **MUST** be trained in their work, particularly in terms of the IT architecture present and the IT systems and applications for which they are responsible. The administrators **MUST** be made familiar with the security provisions that apply in the organisation and are relevant to their work. They **MUST** also be obliged to abide by the relevant data protection laws and any other statutory and internal regulations.

These requirements **MUST** also be met if third parties are assigned administrative tasks.

OPS.1.1.2.A4 Termination of Duties as IT Administrator [Head of Personnel]

If administrators are released from their tasks, all their assigned personal administration credentials **MUST** be withdrawn. It **MUST** be checked which passwords are still known to the employees who are being released from their tasks (e.g. superuser access, emergency users, WLAN passwords). Such passwords **MUST** be changed. All the devices, storage media and means of access (e.g. tokens, chip cards) that were provided to these employees **MUST** be returned.

Furthermore, it **MUST** be checked whether the employees being released from their tasks have been appointed as contact persons for third parties (e.g. in contracts or as an Admin-C entry in Internet domains). In this case, the parties concerned **MUST** be informed and new contact persons **MUST** be appointed. The users of the IT systems and applications concerned **MUST** be informed of the fact that the previous administrator has left.

These requirements **MUST** also be met if third parties have been commissioned with administrative tasks and the employees working there are released from their duties.

OPS.1.1.2.A5 Administration Credentials

Every administrator and every deputy of an administrator **MUST** have a separate, unique administrator ID. The administration rights assigned **MUST** be derived from the requirements of the IT administration tasks assumed in each case.

Administrators **MAY ONLY** perform administrative work using these IDs. They **MAY NOT** be used for routine work for which no advanced authorisations are required (e.g. e-mail communication, research on the Internet). Additional personal, non-privileged accounts **MUST** be created for the administrators for tasks like these.

OPS.1.1.2.A6 Protection of Administrative Credentials

Administration credentials **MUST** be protected appropriately by suitable authentication mechanisms. If passwords are used for this, identical passwords **MAY NOT** be used for IT systems in other protection zones.

Secure protocols **MUST** be used for administration access if this is not performed using a local console. These **MUST** ensure that the communication is encrypted in accordance with the state of the art.

Every login using administration credentials **MUST** be logged so that the time, method and credentials used are transparent.

Standard Requirements

For module OPS.1.1.2 *Proper IT Administration*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

OPS.1.1.2.A7 Regulation of IT Administration Tasks [Head of Personnel]

The competences, tasks and obligations of the administrators **SHOULD** be defined in a binding manner in a work instruction or policy. The division of the work among the different administrators **SHOULD** be performed in such a way that overlapping responsibilities are avoided, but all the tasks which need to be performed are still assigned. The regulations **SHOULD** be updated at regular intervals. The specifications **SHOULD** specifically rule out unauthorised changes performed within the information domain by the administrators, to the extent that the changes exceed the tasks explicitly assigned to them and are not necessary in order to prevent a security incident or failure.

OPS.1.1.2.A8 Administration of Specialised Applications [IT Operation Department]

The basic requirements mentioned in this module **SHOULD** also be implemented consistently for employees with administrative tasks for individual specialised applications. The division of the work between application and system administration **SHOULD** be clearly defined and doc-

umented in writing. Interfaces SHOULD be defined between the persons in charge of system and specialised application administration (e.g. contact persons, communication channels, regular meetings).

In the event of administrative interventions into application operations (e.g. during version changes or maintenance windows), this SHOULD be coordinated with the respective area in advance and take its needs into consideration.

OPS.1.1.2.A9 Sufficient Resources for IT Operations

Sufficient personnel and material resources SHOULD be provided in order to properly handle the administrative tasks at hand. This SHOULD take into account the fact that appropriate capacities must also be available for unforeseeable tasks, particularly for handling and investigating security-relevant events.

Resource planning SHOULD be reviewed regularly (e.g. annually) and adapted to the current requirements.

OPS.1.1.2.A10 Further Education and Information [Head of Personnel]

Appropriate further education and training measures SHOULD be provided for the administrators deployed so that they are always up to date. This SHOULD also consider technical developments that are not currently used but may become important to the organisation in the foreseeable future. The further education measures SHOULD be based on a training schedule and include the entire team so that all the necessary qualifications are represented within the team multiple times.

Administrators SHOULD regularly obtain information regarding the security of the systems, services and protocols they support, especially in connection with current threats and security safeguards.

OPS.1.1.2.A11 Documentation of IT Administration Tasks [IT Operation Department]

System changes SHOULD be documented in an appropriate and transparent form. The documentation SHOULD include:

- which changes have been performed,
- when the changes were performed,
- who performed the changes,
- what the basis and reasons for the changes were.

OPS.1.1.2.A12 Provisions for Maintenance and Repair Work [IT Operation Department]

IT systems SHOULD be maintained at regular intervals. It SHOULD be regulated which security aspects have to be taken into account when performing maintenance and repair work and who is responsible for the maintenance and repair of devices. The employees SHOULD know that maintenance personnel must be supervised when working in-house. Maintenance tasks carried out SHOULD be documented.

OPS.1.1.2.A13 Secure Remote Maintenance [IT Operation Department, Chief Information Security Officer (CISO)]

Remote maintenance SHOULD only be performed if appropriate security safeguards have been implemented. It SHOULD be ensured that remote maintenance access can only be initiated by the local IT system. The performance of remote maintenance SHOULD be logged sufficiently.

Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.1.2 *Proper IT Administration* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.1.1.2.A14 Security Vetting of Administrators (CIA)

An additional security check SHOULD take place in the high-security area to confirm the trustworthiness of employees.

OPS.1.1.2.A15 Division of Administration Activities (CI)

Different administration roles SHOULD be created for partial tasks. When identifying tasks not in scope, the type of data and the existing system architecture SHOULD be taken into consideration.

OPS.1.1.2.A16 Access Restrictions for Administrative Access (CIA)

In the event of increased protection needs, access to administrative interfaces SHOULD be restricted technically by means of filtering and separation measures (i.e. they SHOULD not be available to persons outside of the responsible IT administration team). Administrative access to IT systems in other protection zones SHOULD always be performed using a jump server in the respective security zone. Access attempts from other systems or other security zones SHOULD be rejected.

OPS.1.1.2.A17 Dual Control in IT Administration (CI)

For particularly security-critical systems, access to credentials with administrative authorisations SHOULD be implemented in a way that always requires two employees. In other words, one administrator SHOULD perform the pending administrative tasks under the supervision of a second administrator.

OPS.1.1.2.A18 Consistent Logging of Administrative Activities (CI)

Administrative activities SHOULD be logged whenever possible. For particularly security-critical systems, all administrative access attempts SHOULD be logged consistently and completely. The executing administrators SHOULD not have authorisation to change or delete the recorded log files. The log files SHOULD be stored for a period of time that is appropriate for the protection needs and also makes it possible to investigate subsequent interventions in the system.

OPS.1.1.2.A19 Consideration of High-Availability Requirements (A)

The administrators SHOULD analyse which of the systems and networks they support are subject to high-availability requirements. For these areas, they SHOULD make sure that the components and architectures used, as well as the related operating processes, are appropriate re-

garding the fulfilment of these requirements. Normally, this requires comprehensive high-availability planning.

Additional Information

For more information about threats and security safeguards for module OPS.1.1.2 *Proper IT Administration*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[HVK]	High Availability Compendium: Federal Office for Information Security (BSI), November 2013, https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html , last accessed on 24.08.2018
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.1.1.2 *Proper IT Administration*:

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.35 Coercion, Blackmail or Corruption

G 0.37 Repudiation of Actions

G 0.42 Social Engineering

Elementary Threats Requirements	G 0.14	G 0.16	G 0.21	G 0.22	G 0.27	G 0.29	G 0.30	G 0.31	G 0.32	G 0.33	G 0.35	G 0.37	G 0.42
OPS.1.1.2.A1	X	X	X	X				X	X		X		
OPS.1.1.2.A2										X			
OPS.1.1.2.A3	X	X	X	X		X	X		X		X		X
OPS.1.1.2.A4	X		X	X			X		X		X	X	
OPS.1.1.2.A5	X		X	X			X					X	
OPS.1.1.2.A6	X		X	X			X					X	
OPS.1.1.2.A7	X		X	X		X	X		X				
OPS.1.1.2.A8							X	X	X				
OPS.1.1.2.A9					X			X		X			
OPS.1.1.2.A10								X					
OPS.1.1.2.A11				X			X		X			X	
OPS.1.1.2.A12	X	X	X	X		X	X						X
OPS.1.1.2.A13	X		X	X			X		X			X	
OPS.1.1.2.A14	X	X	X	X			X		X				
OPS.1.1.2.A15			X	X					X		X		X
OPS.1.1.2.A16	X		X	X			X						
OPS.1.1.2.A17	X		X	X	X		X	X	X	X	X	X	X
OPS.1.1.2.A18	X		X	X			X		X			X	
OPS.1.1.2.A19					X					X			



OPS.1.1.3: Patch and Change Management

Description

Introduction

Due to the increasing speed of IT development and users' growing requirements, many public authorities and companies face the task of updating their information technology in a suitable and timely fashion. In practice, vulnerabilities or operational disruptions often prove to have been caused by errors in applying patches and changes (or by failures to apply them at all). Improper or non-existent patch and change management can also quickly result in security vulnerabilities in the individual components, and therefore open up potential points of attack.

In general, the task of patch and change management is to design all changes made to applications, infrastructure, documentation, processes and procedures so that they are manageable and controllable.

Objective

This module shows how to design functional patch and change management in an organisation and how the corresponding process can be controlled and optimised.

Not in Scope

The descriptions in this module focus on IT operations, but can also be implemented in other business processes. Change management refers to the task of planning and controlling changes. Since this process is very elaborate, the standard requirements of the module focus above all on larger information domains. In case of smaller organisations, fulfilment of the standard requirements should be verified; however, the expenses should not outweigh the benefits. Patch management is a partial or special process within change management that focuses on updating software; it must be employed in every case. The individual modules of the SYS and APP layers include additional requirements regarding patch management where required.

Threat Landscape

For module OPS.1.1.3 *Patch and Change Management*, the following specific threats and vulnerabilities are of particular importance:

Poorly Defined Responsibilities

Poorly defined, overlapping or undefined responsibilities could result, for example, in slower categorisation and prioritisation of change requirements, which could then result in the overall delay of distribution of patches and changes. It can also have a serious effect on security if patches and changes are released rashly without performing a test run or considering all the (technical) aspects.

In extreme cases, poorly defined responsibilities may adversely affect the entire organisation or large parts of it. Disruptions in operations affect availability. If security-relevant patches are distributed late (or not at all), confidentiality and integrity may be affected.

Poor Communication in Change Management

If patch and change management is poorly accepted within the organisation or if the people involved communicate poorly, this can lead to processing delays and incorrect decisions related to change requests.

This may reduce the security level, and IT operations may be seriously impaired. In any case, the change process will be inefficient in the event of poor communication because it often requires excessive time and resources. This has adverse effects on the organisation's ability to react and may, in extreme cases, result in vulnerabilities or an inability to attain important business objectives.

Poor Consideration of Business Processes

Inappropriate changes may, amongst other things, impair the smooth handling of business processes or even cause the IT systems involved to fail completely. Even when using the most comprehensive testing procedure, it cannot be ruled out that a change will turn out to be faulty during later production operations.

If, in the course of the change process, the impact, category or priority of a submitted change request is assessed incorrectly regarding the business processes, the organisation may fall short of its desired security level. Such misjudgements are predominantly the result of poor coordination between the persons in charge of IT and the departments involved.

Insufficient Resources for Patch and Change Management

Effective patch and change management requires appropriate personnel, time and financial resources. If suitable employees are not available, for example, the required roles could be staffed with unqualified personnel. This could result in interfaces for certain information (e.g. between IT and the corresponding contact persons in departments) not being created, or the required capacities for the infrastructure of the test and distribution environments not being provided. It is often possible to compensate for shortages of personnel, time and finances during normal operations, but under serious time pressure (e.g. when emergency patches are being installed), these shortages will become more apparent.

Problems in Automating the Distribution of Patches and Changes

In many cases, patches and changes are not distributed manually, but centrally with software support. If such software is used, incorrect patches and changes can be distributed throughout the entire information domain, which can result in a multitude of security problems. This can

be particularly severe if software with vulnerabilities is installed simultaneously on many systems.

If errors only occur occasionally, they can often be remedied manually. However, problems can arise if IT systems are permanently unavailable in the LAN. Field representatives who connect their IT systems to the LAN only sporadically are one such example. If the tool is configured in such a way that the updates are only distributed within a certain period of time and not all IT systems are available in that window, these systems will not be updated.

Poor Recovery Options for Patch and Change Management

If patches or changes are distributed without a recovery option or the recovery routines of the employed software are not suitable and effective, it will not be possible to remedy incorrectly updated software in good time. This may result in the failure of important IT systems and high consequential damage. In addition to the integrity of data, this particularly threatens availability.

Poor Consideration of Mobile End Devices

Mobile end devices pose a particular challenge to change management because their changing places of use and their connection to radio networks mean they are not always included in the automated distribution of patches and changes. Moreover, bandwidth and stable data transmissions are not always guaranteed for mobile end devices. If such devices do not receive special consideration in patch and change management, patches and changes may be distributed incompletely, which requires more time than scheduled and always presents a security risk.

Inadequate Contingency Planning Concept for Patch and Change Management

Patch and change management contributes to the technical implementation of information security in an organisation. The IT systems used by this process must be considered critical for IT operations. For example, this includes the central servers for the distribution of patches and changes, the databases with the current configurations of the IT system and the backup servers for the restoration points. If the server distributing the changes fails, for example, it may be impossible to promptly install recently released critical updates. In addition, the lack of backups of the IT systems' current configurations can mean that the ability to quickly reset important IT components to their original state will no longer be guaranteed in the event of an emergency.

Misjudging the Relevance of Patches and Changes

If changes are prioritised incorrectly, unimportant patches could be installed first, for example. Important patches may thus be installed too late, allowing vulnerabilities to remain for a longer time. Patch and change management is often supported by software-based tools. These tools may also contain software errors and therefore provide insufficient or incorrect information on a change. If the change information provided by a tool of this kind is not verified and checked for plausibility, the actual implementation may deviate from the assumptions made.

Manipulation of Data and Tools in Change Management

Patch and change management often takes place from a central location. Due to its exposed position, it is particularly endangered: if attackers succeed in taking over the servers involved, they could use this central location to distribute manipulated software versions to a large number of IT systems simultaneously. Further points of attack are often created by the fact

that these systems are operated by external partners (outsourcing). Maintenance access may also be configured, allowing attackers to access the central server for distributing changes.

Requirements

The specific requirements of module OPS.1.1.3 *Patch and Change Management* are listed below. As a matter of principle, the *IT Operation Department* is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Administrator, Change Manager, Process Owner, Head of IT

Basic Requirements

For module OPS.1.1.3 *Patch and Change Management*, the following requirements **MUST** be implemented as a matter of priority:

OPS.1.1.3.A1 Concept for Patch and Change Management [Administrator, Process Owner]

If changes to IT components, software or configuration data should be implemented, there **MUST** be specifications that also consider security aspects. All patches and changes **MUST** be suitably planned, approved and documented. Patches and changes **SHOULD** be suitably tested in advance. Patches and changes **SHOULD** be classified according to their importance and urgency and implemented accordingly. If patches and changes are performed, fallback solutions **MUST** be present. In case of large changes, information security management also **MUST** be involved. Overall, it **MUST** be ensured that the desired security level is maintained during and after the implementation of changes.

OPS.1.1.3.A2 Specification of Responsibilities [Head of IT]

Persons in charge of patch and change management **MUST** be specified for all organisational areas. The defined responsibilities **MUST** also be reflected in the access control policy. Moreover, a dedicated change manager **SHOULD** be appointed. All persons involved **MUST** be familiar with the terms of patch and change management, information security and cryptographic procedures.

OPS.1.1.3.A3 Configuration of Auto-Update Mechanisms [Administrator]

The handling of integrated auto-update mechanisms of the employed software **MUST** be defined within the strategy for patch and change management. In particular, it **MUST** be determined how these mechanisms are to be secured and appropriately configured to meet the requirements of the patch management concept. Moreover, new components **SHOULD** be checked to see what type of update mechanisms they have (if any).

Standard Requirements

For module OPS.1.1.3 *Patch and Change Management*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

OPS.1.1.3.A4 Planning the Change Management Process [Change Manager]

A change management process SHOULD be defined; here, organisations may use the change management process of the IT Infrastructure Library (ITIL) as orientation. All changes regarding hardware and software versions and configurations SHOULD be controlled and monitored using the change management process.

OPS.1.1.3.A5 Handling Change Requests [Change Manager]

Requests for changes SHOULD be submitted and processed according to the specified procedure. All requests for changes SHOULD be acquired, documented and then checked by the change manager. Once a request for change has been accepted, it SHOULD be prioritised and categorised. Here, it SHOULD be ensured that the required resources are available for the corresponding priorities.

OPS.1.1.3.A6 Coordination of Change Requests [Change Manager]

If a change is implemented, the relevant coordination process SHOULD consider all relevant target groups. The target groups affected by the change SHOULD be able to comment on the change in a verifiable manner. There SHOULD be a defined procedure to speed up the handling of important requests for changes.

OPS.1.1.3.A7 Integration of Change Management into Business Processes [Change Manager]

The change management process SHOULD be integrated into the business processes. In case of planned changes, the current situation of the affected business processes SHOULD be considered. All relevant departments SHOULD be informed of upcoming changes. There SHOULD be an escalation level whose members make up part of the top management of the organisation and decide on the priority and scheduling of a hardware or software change in case of doubt.

OPS.1.1.3.A8 Secure Use of Tools for Patch and Change Management [Head of IT]

Requirements and framework conditions SHOULD be defined for selecting tools for patch and change management. Furthermore, a specific security policy SHOULD be drawn up for the employed tools.

OPS.1.1.3.A9 Testing and Acceptance Procedures for New Hardware and Software [Head of IT]

New hardware and software SHOULD be tested before being used. Only isolated test systems SHOULD be used for this. There also SHOULD be an acceptance procedure and an approval confirmation for software. The person in charge SHOULD file the approval confirmation at a suitable location in writing. In the event that errors are detected in the software during live operation despite the acceptance and release procedures, there SHOULD be a procedure for troubleshooting.

OPS.1.1.3.A10 Assuring the Integrity and Authenticity of Software Packages [Administrator]

The authenticity and integrity of software packages SHOULD be ensured throughout the patch and change process. To this end, it SHOULD be checked whether checksums or digital signa-

tures are available for the software packages used. Furthermore, it SHOULD be ensured that the programs required for checking are available.

OPS.1.1.3.A11 Continuous Documentation of Information Processing [Head of IT, Change Manager]

Changes SHOULD be documented in all phases, applications and systems. Corresponding rules SHOULD be elaborated for this purpose.

Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.1.3 *Patch and Change Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.1.1.3.A12 Scalability in Change Management (A)

If a tool for change management is used, the implementation speed SHOULD be checked carefully before commissioning. It SHOULD be possible to define break points for stopping the distribution of incorrect changes.

OPS.1.1.3.A13 Measuring the Success of Change Requests (IA)

The change manager SHOULD perform subsequent tests to verify that a change has been successful. For this, the change manager SHOULD select suitable reference systems as quality assurance systems. The results of the subsequent tests SHOULD be documented within the scope of the change process.

OPS.1.1.3.A14 Synchronisation Within Change Management [Change Manager] (CIA)

If organisations make changes to the IT infrastructure, the change management process SHOULD respond accordingly. Suitable mechanisms SHOULD be employed to include devices in the change management process even when they are temporarily or generally unavailable.

Additional Information

For more information about threats and security safeguards for module OPS.1.1.3 *Patch and Change Management*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
---------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

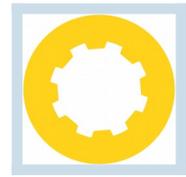
Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.1.1.3 *Patch and Change Management*:

G 0.9 Failure or Disruption of Communication Networks

- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.33 Shortage of Personnel
- G 0.37 Repudiation of Actions
- G 0.39 Malware
- G 0.40 Denial of Service
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.9	G 0.18	G 0.19	G 0.20	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.33	G 0.37	G 0.39	G 0.40	G 0.45	G 0.46
OPS.1.1.3.A1		X													
OPS.1.1.3.A2		X						X		X	X				
OPS.1.1.3.A3	X		X	X	X	X	X		X			X	X		X
OPS.1.1.3.A4		X													
OPS.1.1.3.A5		X		X		X	X	X			X				
OPS.1.1.3.A6		X				X	X	X		X	X				
OPS.1.1.3.A7		X				X	X	X		X	X				
OPS.1.1.3.A8	X		X	X	X	X	X	X	X			X	X	X	X
OPS.1.1.3.A9	X					X	X		X						
OPS.1.1.3.A10			X	X	X				X			X	X		X
OPS.1.1.3.A11		X									X				
OPS.1.1.3.A12		X				X	X	X		X					
OPS.1.1.3.A13		X													
OPS.1.1.3.A14		X						X							



OPS.1.1.4: Protection Against Malware

Description

Introduction

Malware refers to programs that perform harmful functions on an IT system, usually without the knowledge or consent of the user or owner of the IT system. These functions can cover a wide area, ranging from potential espionage and extortion (using so-called ransomware) to the sabotage and destruction of information, or even devices.

Basically, malware may occur on all operating systems and IT systems. In addition to classic IT systems such as clients and servers, this also includes mobile devices such as smartphones. Today, network components like routers and industrial control systems – and even IoT devices such as networked cameras – are also frequently threatened by malware.

On classic IT systems, malware is distributed mainly via e-mail attachments, manipulated web pages (drive-by downloads) or storage media. Smartphones are usually infected by installing malicious apps; drive-by downloads are also possible. Furthermore, open network interfaces, incorrect configurations and software vulnerabilities are frequent points of entry on all IT systems.

This module uses the term “virus protection program”. Here, “viruses” are a synonym for all types of malware. This means a program for protecting against any type of malware.

Objective

This module describes the procedure of creating and implementing protection against malware to effectively guard an organisation against malware.

Not in Scope

This module describes the general requirements for protection against malware. Specific requirements for protecting particular IT systems in the organisation against malware are included in the relevant modules, particularly in the SYS layer (e.g. in SYS.2.2.3 *Windows 10 Clients*). If identified malware results in a security incident, the requirements of the module DER.2.1 *Security Incident Handling* should be considered. The requirements of the module DER.2.3 *Clean-Up of Extensive Security Incidents* help in removing identified malware and re-establishing a cleaned state.

Threat Landscape

The following specific threats and vulnerabilities are of particular importance for module OPS.1.1.4 *Protection Against Malware*:

Software Vulnerabilities and Drive-By Downloads

If IT systems are not protected sufficiently against malware (which requires, for example, that patches be installed in good time and protection mechanisms of application programs such as browsers be configured correctly), software vulnerabilities can be exploited for executing malicious code. In the case of so-called drive-by downloads, it may be enough to visit a malicious website, for example. A vulnerability in the browser or in an installed plug-in such as Java or Adobe Flash can then be exploited to infect the IT system and provide the attacker with comprehensive control, as well as access to the network of an organisation. IT systems that are not updated regularly (e.g. many smartphones) are at particular risk in this regard.

Extortion Through Ransomware

Ransomware is a widespread type of malware. It encrypts the data of the infected IT system and, in many cases, further data that can be accessed (e.g. through network shares). Usually, the attackers use encryption methods that cannot be reversed without the corresponding key as a means of extorting large sums of money from their victims. If there is no effective protection against malware and there are no supplemental precautions (such as backups), the availability of information could be significantly limited and serious financial and reputation damage could be suffered.

Targeted Attacks and Social Engineering

Organisations are often attacked by customised malware. In such cases, supervisors (for example) are tricked into opening harmful e-mail attachments by methods of social engineering. Customised malware often cannot be detected immediately by virus protection programs. Also the Human Resources department of an organisation can be the target such as by electronically sending malicious application documents. If the attacker has managed to infect an IT system using such methods, they may infiltrate other areas of the organisation and steal, manipulate or destroy information.

Infections Through Mobile Storage Media and Other USB Devices

Mobile storage media (i.e. USB devices) can also become a point of entry for malware if there is not sufficient user awareness. An attacker may place malicious USB pen drives on the property of an organisation, for example, and unwary users may connect them to IT systems. In addition to devices that can be immediately identified as mobile storage media, other USB devices can also have malicious functions (by simulating removable media or keyboard entries, for example). A USB mouse, for example, can also act as a storage medium when connected to the IT system. If there is insufficient protection against malware, an attacker may use this route to gain access to the network and the data of the organisation.

Botnets

Malware may recruit the IT systems of an organisation into so-called botnets. Attackers, who often control thousands of systems in a botnet, can use them to send spam or start distributed denial-of-service attacks (DDoS) on third parties. Even though the affected organisation itself

may not be damaged directly, this may have negative effects regarding the availability and integrity of its own services and IT systems, and may even result in legal problems.

Infection of Production Systems and IoT Devices

In addition to classic IT systems, devices that are not initially considered to be obvious targets are increasingly being attacked by malware. For example, an attacker may infect a surveillance camera accessible via the Internet for spying. However, even a networked light bulb or a coffee machine with app control may serve as points of entry into the network of the organisation or as part of a botnet unless these devices are protected sufficiently against malware. Networked production systems or industrial controls can also be manipulated or even destroyed by malware, which may result in downtime and further risks to the organisation and its employees (e.g. due to fire).

Requirements

The specific requirements of module OPS.1.1.4 *Protection Against Malware* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User, Process Owner

Basic Requirements

For module OPS.1.1.4 *Protection Against Malware*, the following requirements **MUST** be implemented as a matter of priority:

OPS.1.1.4.A1 Creating a Concept for Protection Against Malware

A concept on which IT systems must be protected against malware **MUST** be drawn up. Furthermore, it **MUST** be specified how protection is to be implemented. If no reliable protection is possible, the identified IT systems **SHOULD NOT** be operated. The concept **SHOULD** be documented in an understandable manner.

OPS.1.1.4.A2 Using System-Specific Protection Mechanisms

The protection mechanisms provided by the IT systems used, as well as by the operating systems and applications used on them, **MUST** be checked to enable or support protection against malware. Such mechanisms **MUST** be used unless there is at least an equal substitute or there are good reasons against such use. If they are not used, this **SHOULD** be explained and documented.

OPS.1.1.4.A3 Selecting a Virus Protection Program for End Devices

A protection program **MUST** be selected and installed for the actual intended purpose according to the operating system used, the other protection mechanisms present and the availability of suitable virus protection programs. **ONLY** products with services and support that meet the

organisation's needs MAY be used for the enterprise area. Products for purely home-based users or products without manufacturer support MUST NOT be used for professional production operations. If the cloud functions of such products are used, they MUST NOT be in conflict with any serious and verifiable aspects of data protection or confidentiality.

OPS.1.1.4.A4 Selecting a Virus Protection Program for Gateways and IT Systems for Data Exchange [Process Owner]

A suitable virus protection program MUST be selected and installed for gateways and IT systems used for data exchange. ONLY products with services and support that meet the organisation's needs MAY be used for the enterprise area. Products for purely home-based users or products without manufacturer support MUST NOT be used for professional production operations. If the cloud functions of such products are used, they MUST NOT be in conflict with any serious and verifiable aspects of data protection or confidentiality.

OPS.1.1.4.A5 Operating Virus Protection Programs

The virus protection program MUST be configured appropriately for its operational environment. The focus SHOULD be on detection performance unless data protection or performance reasons are more important in an individual case. If security-relevant functions of the virus protection program are not used, this SHOULD be explained and documented. In the case of protection programs that are specially optimised for desktop virtualisation, it SHOULD be transparent whether certain detection procedures have been omitted in favour of performance.

OPS.1.1.4.A6 Updating Virus Protection Programs and Signatures

The scan engine of the virus protection program, as well as its malware signatures, MUST be updated regularly on the corresponding IT systems. The frequency of quality-assured signature updates MUST conform to the manufacturer's recommendations.

Updates to new program versions SHOULD be carried out promptly after publication. The change documentation of the manufacturer SHOULD be checked for relevant changes upon every update of the virus protection program. After installing the update, the configuration settings MUST be checked and compared against the documented specifications.

OPS.1.1.4.A7 User Awareness and Obligations [User]

Users MUST be informed regularly of the threats posed by malware. They MUST comply with the basic rules of conduct to reduce the risk of malware infection. Files from untrusted sources SHOULD NOT be opened.

Standard Requirements

For module OPS.1.1.4 *Protection Against Malware*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

OPS.1.1.4.A8 Using Cloud Services

Cloud services for improving the detection performance of the virus protection programs SHOULD be used. Here, the corresponding specifications from the requirements of OPS.1.1.4.A3 *Selecting a Virus Protection Program for End Devices* and OPS.1.1.4.A4 *Selecting a Virus Protection Program for Gateways and IT Systems for Data Exchange* MUST be considered.

OPS.1.1.4.A9 Reporting Malware Infections [User]

The virus protection programs used SHOULD automatically block and report any malware infection. The automatic report SHOULD be sent to a central location. The employees responsible SHOULD then decide how to proceed further based on the current situation. Irrespective of an automatic report, however, the user SHOULD also notify the known contact persons if there is a suspected malware infection. The procedure in case of reports and alarms of the virus protection programs SHOULD be planned, documented and tested. In particular, the actions to be taken in case of a confirmed infection SHOULD be specified.

Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.1.4 *Protection Against Malware* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.1.1.4.A10 Using Special Analysis Environments (CIA)

Automated analyses in a special test environment (based on sandboxes, or separate virtual or physical systems) SHOULD also be used for assessing suspicious data.

OPS.1.1.4.A11 Using Several Scan Engines (CIA)

To improve the detection performance, virus protection programs with several alternative scan engines SHOULD be used for IT systems that require special protection (e.g. gateways and IT systems for data exchange).

OPS.1.1.4.A12 Using Storage Media Locks (CIA)

Before connecting storage media from third parties to the IT systems of the organisation, the media SHOULD be checked in a storage media lock.

OPS.1.1.4.A13 Handling Untrusted Files (CIA)

If it is necessary to open untrusted files, this only SHOULD be performed on an isolated IT system. In this system, the corresponding files SHOULD be converted into a secure format or printed, for example, if doing so will reduce the risk of a malware infection.

OPS.1.1.4.A14 Selecting and Using Cyber Security Products to Thwart Targeted Attacks (CIA)

In case of increased protection needs and a corresponding threat landscape, the use and added value of products and services that offer an extended scope of protection compared to normal virus protection programs (such as executing files in special analysis environments, hardening of clients or encapsulation of processes) SHOULD be considered. Before making a purchase decision, the effects of this protection and its compatibility with the organisation's own IT environment SHOULD be tested.

OPS.1.1.4.A15 External Consulting (CIA)

When drawing up a concept for protection against malware, external support SHOULD be used if the organisation's own expertise or knowledge of the market is not sufficient. Protection products in complex IT infrastructures SHOULD only be implemented by experienced experts to avoid performance problems within the IT systems and networks and to incorporate

the protection against malware into an overall concept in a sensible manner. After protection programs are installed, the configuration SHOULD be reviewed by external experts.

Additional Information

For more information about threats and security safeguards for module OPS.1.1.4 *Protection Against Malware*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[ISFTS1]	The Standard of Good Practice for Information Security: Area TS2 Cryptography, Information Security Forum (ISF), June 2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.1.1.4 *Protection Against Malware*:

G 0.14 Interception of Information / Espionage

G 0.19 Disclosure of Sensitive Information

G 0.23 Unauthorised Access to IT Systems

G 0.32 Misuse of Authorisation

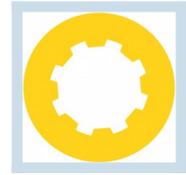
G 0.36 Identity Theft

G 0.39 Malware

G 0.42 Social Engineering

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.14	G 0.19	G 0.23	G 0.32	G 0.36	G 0.39	G 0.42	G 0.46
OPS.1.1.4.A1	X	X	X	X	X	X	X	X
OPS.1.1.4.A2	X	X	X	X	X	X		X
OPS.1.1.4.A3	X	X	X	X	X	X		X
OPS.1.1.4.A4	X	X	X	X	X	X		X
OPS.1.1.4.A5	X	X	X	X	X	X	X	X
OPS.1.1.4.A6	X	X	X	X	X	X	X	X
OPS.1.1.4.A7	X	X	X	X		X		X
OPS.1.1.4.A8	X	X	X	X	X	X	X	X
OPS.1.1.4.A9	X	X	X	X	X	X		X
OPS.1.1.4.A10	X	X	X	X	X	X		X
OPS.1.1.4.A11	X	X	X	X	X		X	X
OPS.1.1.4.A12	X	X	X	X	X	X		X
OPS.1.1.4.A13	X	X	X	X	X	X		X
OPS.1.1.4.A14	X	X	X	X	X	X		X
OPS.1.1.4.A15	X	X	X	X	X	X	X	X



OPS.1.1.5: Logging

Description

Introduction

To ensure reliable IT operation, IT systems and applications should log all or select events relevant for operation and security (i.e. store them automatically and provide them for assessment). Logging is used in many organisations in order to be able to promptly identify hardware and software problems and resource bottlenecks. However, security problems and attacks on the operated services can also be comprehended on the basis of log data. Through forensic examination, evidence can be secured in such data after an attack on IT systems has become known.

In each information domain, log data is locally generated by a multitude of IT systems and applications. However, in order to get a complete overview of the information domain, the logging information generated by various IT systems and applications can be sent to a dedicated logging infrastructure for central storage. Only then can the log data be selected, filtered and analysed systematically at one location.

Objective

This module contains requirements for implementing the logging of as many security-relevant events as possible. The aim is to securely acquire and store all data relevant for this, provide it in a suitable manner for assessment and ensure its proper disposal.

Not in Scope

The present module only considers overarching aspects that are required for appropriate logging. The logging of specific IT systems or applications is not dealt with here, but is described in the relevant modules.

In many operating systems or applications, logging functions are already present or can be integrated through additional products. The underlying operating system must be protected to safeguard these functions and the stored log data. However, this is not covered in this module. The operating-system-specific modules must be implemented in this regard (e.g. *SYS.1.1 General Server* and *SYS.2.1 General Client*).

This module should also be differentiated from the detection of security incidents (see *DER.1 Detecting Security-Relevant Events*) and related response efforts (*DER.2.1 Security Incident Handling*). These aspects are not (or only marginally) covered in module *OPS.1.1.5 Logging*.

Specifications on how to handle personal data are included in module *CON.2 Data Protection*. The duration and scope of log data archiving is also explained in module *OPS.1.2.2 Archiving*.

Threat Landscape

For module OPS.1.1.5 *Logging*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Logging

Within an information domain, there are often IT systems and applications with default settings in which logging has not been enabled. Sometimes, individual IT systems and applications are not able to perform logging at all. In both cases, important information may be lost and it may be impossible to detect attacks in time. However, this is also possible if logging is used for individual IT systems, but the logs are not combined at a central location. In information domains without centralised logging, it is difficult to ensure that the relevant logged information of all IT systems will be maintained and analysed.

Furthermore, log data must contain meaningful information. The events to be logged depend, among other things, on the protection needs of the corresponding IT systems and applications. If this is disregarded (e.g. by only using the default settings of the IT systems and applications for logging), this may result in particularly relevant security events not being logged. Attacks may not be detected as a result.

Incorrect Selection of Relevant Log Data

Log data often provides important information that facilitates the detection of IT security incidents. Selecting the relevant messages from the large number of different log events is a particular challenge. This is because numerous messages are only informative and divert attention from the messages that are actually important. If too many log messages are selected, the wealth of information can hardly be analysed and requires huge amounts of time.

Furthermore, log data can be discarded or overwritten if the internal memory, the hard drive capacity of the IT system or the logging infrastructure is insufficient. If this results in too few relevant log messages being recorded, security-critical incidents may remain undetected.

Lack of Time Synchronisation During Logging

If the time is not synchronised on all IT systems within an information domain, the log data may not correlate or the correlation may result in erroneous statements due to the lack of a common basis among the different time stamps of events. It is thus harder to assess the acquired log data where there is no time synchronisation, particularly if the data is stored on a central log server. Furthermore, erroneous time synchronisation (or none at all) may make it impossible to use logs in securing evidence.

Poor Planning of Logging

If logging is not sufficiently planned, IT systems or applications may not be monitored, and security-relevant events may not be identified and appropriately dealt with as a result. Data protection infringements cannot be traced either.

Loss of Confidentiality and Integrity Regarding Log Data

Some IT systems in an information domain generate log data (such as user names, IP addresses, e-mail addresses and computer names) that can be associated with specific persons. Such information can be copied, intercepted and manipulated if it is not encrypted and securely

stored. This may result in attackers accessing confidential information or manipulated log data being used to deliberately disguise security incidents. Furthermore, if an attacker obtains a large amount of log data, they may use it to reveal the internal structure of the information domain and carry out more targeted attacks.

Incorrectly Configured Logging

If logging in IT systems is incorrectly configured, important information will be recorded improperly (or not at all). It is also possible that incorrect or excessive information will be logged. For example, personal data may be logged and stored without authorisation, and the organisation may thereby infringe on legal regulations.

Due to incorrectly configured logging, log data may also be available in inconsistent or proprietary formats. In such cases, the logs may be difficult to assess and IT security incidents may remain undetected.

Failure of Data Sources

If IT systems in an information domain no longer provide the required log data, it will no longer be possible to appropriately detect security incidents. Errors in hardware and software, as well as incorrectly administered IT systems, can be the cause of failures of data sources. In particular, if the failure of data sources is not detected, this may result in a false perception of the security situation in the organisation. Attackers could thus remain undetected for a long period of time and intercept business-critical information or manipulate production systems, for example.

Insufficiently Dimensioned Logging Infrastructure

Due to complex information domains and wide-ranging attack scenarios, the requirements on logging are increasing because a very large amount of log data must be stored and processed. Moreover, it is customary to increase the intensity of logging when security incidents occur. However, if the logging infrastructure is not designed for this, the log data stored may be incomplete. As a result, security-relevant events will be assessed insufficiently (or not at all) and security incidents will remain undetected.

Requirements

The specific requirements of module OPS.1.1.5 *Logging* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are fulfilled and verified according to the security concept defined.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO), Process Owner, Head of IT

Basic Requirements

For module OPS.1.1.5 *Logging*, the following requirements **MUST** be implemented as a matter of priority:

OPS.1.1.5.A1 Drawing Up a Security Policy for Logging [Chief Information Security Officer (CISO), Process Owner]

A specific security policy that transparently describes requirements and specifications on how to securely plan, design and operate logging **MUST** be drawn up on the basis of the organisation's general security policy. The policy **MUST** specify how and where logging is to be performed and what is to be logged. In this regard, the type and scope of logging **SHOULD** be based on the protection needs of the information.

The policy **MUST** be drawn up by the CISO together with the process owners. It **MUST** be known to all employees in charge of logging and **MUST** represent the basis for their work. If the policy is changed or there are deviations from the requirements, this **MUST** be agreed with the CISO and documented. The correct implementation of the policy **MUST** be regularly reviewed. The results **MUST** be documented.

OPS.1.1.5.A2 Defining Roles and Responsibilities [Head of IT]

Persons in charge **MUST** be appointed for the IT systems and applications defined as relevant in the logging policy (see OPS.1.1.5.A1 *Drawing Up a Security Policy for Logging*). They **MUST** ensure compliance with the logging policy.

OPS.1.1.5.A3 Configuring Logging at the System and Network Level

All security-relevant events of IT systems and applications **MUST** be logged. If the IT systems and applications defined as relevant in the logging policy have a logging function, it **MUST** be used. When setting up logging, the manufacturer's specifications for the relevant IT systems or applications **MUST** be considered. It **MUST** be verified in bullet point form and at reasonable intervals that the logging still works correctly. The intervals **MUST** be defined in the logging policy. If events relevant for operation and security cannot be logged on an IT system, further IT systems **MUST** be integrated for logging (e.g. of events at the network level).

OPS.1.1.5.A4 Time Synchronisation of IT Systems

The system time of all logging IT systems and applications **MUST** always be synchronous. It **MUST** be ensured that the date and time formats of the log files are uniform. More information in this regard can be found in module NET.1.2 *Network Management*.

OPS.1.1.5.A5 Complying with Legal Framework Conditions [Chief Information Security Officer (CISO)]

The legal regulations of the current laws on federal/state data protection **MUST** be complied with (see CON.2 *Data Protection*) during logging. Moreover, any personal rights and/or rights of co-determination of the Employee Representatives **MUST** be observed. Compliance with all further relevant legal regulations **MUST** also be ensured. Log data **MUST** be deleted in accordance with a specified process. Technical provisions **MUST** prevent log data being deleted or changed in an uncontrolled manner.

Standard Requirements

For module OPS.1.1.5 *Logging*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

OPS.1.1.5.A6 Basic Structure of a Centralised Logging Infrastructure

In larger information domains in particular, all collected security-relevant log data SHOULD be stored at a central location. To this end, a central logging infrastructure by means of a log server system SHOULD be designed and placed in a network segment created for this purpose. The log server system SHOULD always follow the pull principle in obtaining the log data from IT systems and applications. If this is not supported by IT systems and applications, the log data SHOULD be collected on upstream IT systems and picked up there by the log server system. The communication links required for this SHOULD be established restrictively.

In addition to the security-relevant events (see OPS.1.1.5.A3 *Configuring Logging at the System and Network Level*), a central logging infrastructure SHOULD also log general operational events indicating an error, such as:

- the absence of log data or unavailability of a logging IT system
- operational events indicating an extraordinary load, including on individual services

The logging infrastructure SHOULD be sufficiently dimensioned so that scaling by means of extended logging can be taken into consideration. To this end, sufficient technical, financial and personnel resources SHOULD be available. If the logging infrastructure is to be created and operated externally, a specialised service provider SHOULD be commissioned.

OPS.1.1.5.A7 Secure Administration of Logging Servers

The log server domain SHOULD only be administrated via a separate management network (out-of-band management). An access control policy SHOULD be drawn up for administration access. Only those administrators with special responsibility for this task SHOULD access the logging servers (see OPS.1.1.5.A2 *Defining Roles and Responsibilities*).

OPS.1.1.5.A8 Archiving of Log Data

An archiving concept SHOULD be created for log data. Here, the legally required regulations SHOULD be considered and documented in the concept (see also OPS.1.2.2 *Archiving*).

OPS.1.1.5.A9 Providing Log Data for Assessment

The collected log data SHOULD be filtered, normalised, aggregated and correlated using a logging application. The log data processed this way SHOULD be made available in a suitable manner so that it can be assessed. The logging applications SHOULD have corresponding interfaces for the assessment programs so that the data can be assessed automatically. It SHOULD be ensured that the security requirements defined in the logging policy are complied with when performing an assessment. Operational and internal agreements SHOULD also be taken into consideration when the data is made available. The log data SHOULD be stored in its original form.

OPS.1.1.5.A10 Access Protection for Log Data

All log data SHOULD be stored in a way that prevents unauthorised access. Furthermore, an access concept specifying who may access which logged data SHOULD be drawn up. Here, the authorisations SHOULD be as restrictive as possible.

Basically, it SHOULD be ensured that the log data can be accessed only if security-relevant incidents need to be investigated. Here, the method specified in module DER.1 *Detecting Security-Relevant Events* SHOULD be used. Such access SHOULD be documented.

Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.1.5 *Logging* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.1.1.5.A11 Increasing the Scope of Logging (CIA)

In case of increased protection needs of applications or IT systems, the quantity and type of the logged events SHOULD be extended so that security-relevant incidents can be documented as completely as possible.

In order to facilitate real-time assessment of log data, the logging IT systems and applications SHOULD store the log data centrally at shorter time intervals (see also OPS.1.1.5.A6 *Basic Structure of a Centralised Logging Infrastructure*). Logging SHOULD enable assessment of the entire information domain.

Applications and IT systems that do not allow for central logging SHOULD NOT be used in case of increased protection needs.

OPS.1.1.5.A12 Encryption (CI)

Log data SHOULD be encrypted for secure transfer. Furthermore, all stored logs SHOULD be digitally signed. Archived log data and log data stored outside the logging infrastructure should also always be stored in an encrypted manner. Further information and requirements on this are included in module CON.1 *Crypto Concept*.

OPS.1.1.5.A13 Highly Available Logging Systems [Chief Information Security Officer (CISO)] (A)

In case of increased protection needs, a highly available logging infrastructure SHOULD be established.

Additional Information

For more information about threats and security safeguards for module OPS.1.1.5 *Logging*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology-Security techniques-Information security management systems-Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
---------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 15.11.2017

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.1.1.5 *Logging*:

- G 0.9 Failure or Disruption of Communication Networks
- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.37 Repudiation of Actions
- G 0.38 Misuse of Personal Information
- G 0.40 Denial of Service
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G0.9	G0.14	G0.15	G0.18	G0.19	G0.21	G0.22	G0.23	G0.25	G0.26	G0.29	G0.30	G0.31	G0.32	G0.37	G0.38	G0.40	G0.45	G0.46
OPS.1.1.5.A1				X							X					X			
OPS.1.1.5.A2				X								X		X					
OPS.1.1.5.A3	X								X	X			X						
OPS.1.1.5.A4													X						X
OPS.1.1.5.A5											X					X			
OPS.1.1.5.A6	X			X		X	X	X			X	X						X	X
OPS.1.1.5.A7			X				X	X				X							X
OPS.1.1.5.A8				X			X				X							X	X
OPS.1.1.5.A9										X	X		X						
OPS.1.1.5.A10		X			X							X		X		X			X
OPS.1.1.5.A11						X		X	X	X			X		X			X	
OPS.1.1.5.A12		X	X		X		X											X	X
OPS.1.1.5.A13	X								X	X							X	X	



OPS.1.1.6: Software Tests and Approvals

Description

Introduction

The use of IT for dealing with certain tasks requires that computerised data processing work as perfectly as possible, as the individual results can no longer be checked in most cases. That is why it is verified within the scope of software tests whether the software is working without failure. To this end, the software must provide the required function reliably and, moreover, must not have any undesired side effects. With the subsequent approval of the software by the relevant organisational unit, basic permission is granted to use the software in the organisation's production environment. At the same time, this organisational unit assumes responsibility for the IT process supported by the software.

Software can be tested at different stages of its lifecycle. For example, software tests can already become necessary during development, before approval for production operation or within the scope of patch and change management. The software tests and approvals must be performed both for in-house developments and when using standard software.

This module describes the test and approval process for self-developed or adapted software, as well as for standard software. The test and approval process is characterised by the fact that it can be performed several times depending on the result.

Objective

By implementing this module, the organisation can ensure that employed software meets the technical and organisational requirements and the present protection needs of the whole organisation, or individual organisational units thereof. Here, an essential partial aspect involves the systematic and methodical checking of security-critical software for existing vulnerabilities.

Not in Scope

Whilst module CON.8 *Software Development* refers to the software development process and the software tests it requires, this module describes the special requirements of test and approval management. Test and approval management refers not solely to internally developed software or software developed on behalf of the customer, but also to testing and approval in the context of CON.4 *Selection and Use of Standard Software* and APP.1.1 *Office Products*.

Different professional methods are used for software testing. The procedure in penetration tests is described in more detail in module DER.3.3 *Penetration Tests*.

Software tests can also become part of patch or change management. This is further specified in module OPS.1.1.3 *Patch and Change Management*.

Threat Landscape

The following specific threats and vulnerabilities are of particular importance for module OPS.1.1.6 *Software Tests and Approvals*:

Incomplete Implementation of Customer Requirements

If the requirements are incorporated in an incomplete or incorrect manner or the parties involved in software development or purchasing (e.g. the customer and the contractor) communicate insufficiently, the requirements of the customer may not be met completely. This may result in vulnerabilities in the software. For example, if the requirements of the customer need to be incorporated after the fact, software development projects could be delayed, which may result in financial damage.

Insufficient Training of Developers and Software Testers

It is often assumed that qualified developers and software testers have sufficient knowledge of testing and approval software due to their training. As a result, developers and software testers are often insufficiently trained on new developments in their subject area or on the software's field of use. This lack of awareness may result in serious security problems, such as if the programming uses functions and methods that have already been classified as insecure, but the developers are not yet aware of this fact.

Software Testing with Production Data

Software tests with production data or during production operations are required because the function and performance of the product can only be assessed with production data. Often, developers see the developed product differently; for example, they have another security awareness, rely too much on the developed software, and cannot assess correctly the possible impact of problems.

Although software tests with production data are necessary, this may result in security problems. In particular, confidential production data for the software tests may be accessed by unauthorised employees or third parties commissioned with performing the software test.

Software tests during production operations could severely disrupt these operations. Malfunctions of the software to be tested could impact other applications and IT systems, which would be severely disrupted by this. If "original" production data (rather than copies of the data) is used for testing during production operations, it could be inadvertently changed or deleted.

Non-Existent or Insufficient Testing Procedure

If new software is tested insufficiently (or not at all) and approved without installation specifications, errors in the software may remain undetected. Moreover, it is possible that mandatory installation parameters will not be detected or considered as a result.

The software and installation errors not detected due to non-existent or inadequate software testing procedures pose a significant threat to the organisation's IT operations. For example, data can be lost if an update of a database management system is installed without previous testing.

Non-Existent or Insufficient Approval Procedure

A non-existent or insufficient approval procedure may result in the use of software that has not been technically approved. For example, the software may include functions that it should not have, or lack others that are required. Furthermore, the software can be incompatible with other applications.

Inadequate or Non-Existent Documentation of Tests and Test Results

Usually, software can be approved as soon as all tests have been performed and no deviations have been detected. However, if the documentation of the software tests is incomplete, it will not be possible later on to verify what was tested. If detectable software errors or missing functions have been documented insufficiently and thus have not been considered for approval, such deviations may inadvertently delete or change the production data to be processed and other IT systems and applications may be impaired.

Inadequate or Non-Existent Documentation of Approval Criteria

If approval criteria are not clearly communicated, this may result in approval being granted prematurely, or not being granted even though it could be. On the one hand, this may lead to the approval of versions with undetected software errors, which may disrupt the production operation. On the other hand, it may delay the project and thus lead to financial damage.

Requirements

The specific requirements of module OPS.1.1.6 *Software Tests and Approvals* are listed below. As a matter of principle, the Head of IT is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of IT
Further Roles	Head of Personnel, Human Resources Department, Data Protection Officer, IT Operation Department, Tester, Process Owner, Head of IT

Basic Requirements

For module OPS.1.1.6 *Software Tests and Approvals*, the following requirements **MUST** be implemented as a matter of priority:

OPS.1.1.6.A1 Planning of Software Tests

Before software tests can be performed, the framework conditions for such tests **MUST** be specified within the organisation in accordance with the protection needs, organisational units, technical possibilities and test environments. The software tests **MUST** be based on the information in the requirements specification.

When selecting the test cases, it **MUST** be ensured that they are as representative as possible for the functions to be tested.

OPS.1.1.6.A2 Performing Functional Software Tests [Tester]

Functional software tests **MUST** be performed to verify the complete and proper function of the software. The functional software tests **MUST** be performed such that they do not impair production operation.

OPS.1.1.6.A3 Assessing the Test Results [Tester]

The results of the software tests **MUST** be assessed. A gap analysis **SHOULD** be performed using the defined specifications. The assessment **MUST** be documented.

OPS.1.1.6.A4 Software Approval [Process Owner]

The technical organisational unit **MUST** approve the software as soon as the software tests have been performed successfully. The approval **MUST** be documented by means of an approval confirmation.

The approving organisational unit **MUST** verify whether the software has been tested in accordance with the requirements. The results of the software tests **MUST** match the previously specified expectations. It **MUST** also be verified whether compliance with legal or organisational specifications has been ensured.

OPS.1.1.6.A5 Performing Non-Functional Software Tests [Tester]

Non-functional tests **MUST** be performed. In particular, security-specific software tests **SHOULD** be performed if the application includes security-critical functions. Both the test cases carried out and the test results **SHOULD** be documented.

Standard Requirements

For module OPS.1.1.6 *Software Tests and Approvals*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

OPS.1.1.6.A6 Orderly Instruction of Software Testers [IT Operation Department, Process Owner]

The IT Operation Department **SHOULD** inform software testers of the test types to be performed and the software areas to be tested. Furthermore, the software testers **SHOULD** be informed of the use cases and possible further requirements of the software.

OPS.1.1.6.A7 Selecting Software Testers [Human Resources Department, Head of IT]

Particular selection criteria **SHOULD** be considered when selecting the software testers. These persons **SHOULD** have the required professional qualification. They **SHOULD** have sufficient knowledge of the programming language to be tested, the development environment and the test methods to be used.

In public institutions and organisations subject to the security support scheme, it **SHOULD** be verified whether security vetting is necessary.

OPS.1.1.6.A8 Further Training and Continuing Education of Software Testers [Head of Personnel]

The software testers SHOULD be trained in accordance with the module *ORP.3 Awareness and Training*. Procedures for informing software testers of new developments relevant for their corresponding tasks SHOULD be established.

OPS.1.1.6.A9 Procurement of Test Software [IT Operation Department, Tester]

Test software to be purchased SHOULD be acquired in accordance with a requirements catalogue. It SHOULD also be subject to the test and approval process. It SHOULD be verified whether the assistance and support services of the software manufacturer are sufficient.

OPS.1.1.6.A10 Drawing Up an Acceptance Plan

The acceptance plan SHOULD document the test types to be performed, test cases and the expected results. Furthermore, the acceptance plan SHOULD include the approval criteria. The procedure for refusing approval SHOULD be defined.

OPS.1.1.6.A11 Using Anonymised or Pseudonymised Test Data [Data Protection Officer, Tester]

Only anonymised or pseudonymised test data SHOULD be used for software tests. If the production data includes references to persons, the organisations SHOULD only use anonymised test data. If references to persons could be derived from the test data, the Data Protection Officer and, if applicable, the Employee Representatives SHOULD be consulted.

OPS.1.1.6.A12 Performing Regression Tests [Tester]

If software tests are to be performed after changing the software, regression tests SHOULD be performed. Regression tests SHOULD be performed completely. Any omission of test cases SHOULD be explained and documented. The test cases carried out and the test results SHOULD be documented.

OPS.1.1.6.A13 Separating the Test and Quality Management Environment from the Production Environment [IT Operation Department]

Software SHOULD only be tested in a test and quality management environment intended for this purpose. The test and quality management environment SHOULD be operated separately from the production environment. The architectures and mechanisms used in the test landscape SHOULD be documented. The quality management environment SHOULD be adapted to the production environment. Procedures for handling the test landscape after completion of the software tests SHOULD be documented.

Requirements in Case of Increased Protection Needs

Generic suggestions for module *OPS.1.1.6 Software Tests and Approvals* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.1.1.6.A14 Performing Penetration Tests [Tester] (CIA)

Penetration tests SHOULD be performed as a test method for applications and/or IT systems with increased protection needs. A penetration test concept SHOULD be drawn up. In addition to the deployed test methods, the penetration test concept SHOULD document the success criteria.

The penetration test SHOULD be performed in accordance with the framework conditions of the penetration test concept. The vulnerabilities detected during the penetration test SHOULD be classified and documented.

Additional Information

For more information about threats and security safeguards for module OPS.1.1.6 *Software Tests and Approvals*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[29119]	ISO/IEC/IEEE 29119-2:2013: Software and systems engineering - Software testing - Part 2: Test processes, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, September 2013
[BSIPEN]	Study - A Penetration Testing Module: Federal Office for Information Security (BSI), November 2003, https://www.bsi.bund.de/DE/Publikationen/Studien/Pentest/index_hm.html , last accessed on 05.10.2018
[BSIWEB]	BSI-Leitfäden zur Entwicklung sicherer Webanwendungen [BSI Guides for developing secure web applications]: Federal Office for Information Security (BSI), 2013, https://www.bsi.bund.de/DE/Publikationen/Studien/Webanwendungen/index_hm.html , last accessed on 05.10.2018
[CVSS]	Common Vulnerability Scoring System (CVSS): FIRST, https://www.first.org/cvss , last accessed on 05.10.2018
[GLEN]	The Art of Software Testing: Glenford J. Myers, Corey Sandler, Tom Badgett, Third Edition, John Wiley & Sons, November 2011
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nist-pubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 30.08.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.1.1.6 *Software Tests and Approvals*:

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.38 Misuse of Personal Information

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.28	G 0.29	G 0.30	G 0.31	G 0.38	G 0.42	G 0.43	G 0.45	G 0.46
OPS.1.1.6.A1	X													
OPS.1.1.6.A2	X													
OPS.1.1.6.A3	X													
OPS.1.1.6.A4								X						
OPS.1.1.6.A5		X	X	X	X	X				X		X	X	X
OPS.1.1.6.A6	X													
OPS.1.1.6.A7	X						X							
OPS.1.1.6.A8										X				
OPS.1.1.6.A9									X		X			
OPS.1.1.6.A10	X	X	X	X	X	X	X	X		X		X	X	X
OPS.1.1.6.A11		X								X				
OPS.1.1.6.A12		X	X	X	X	X				X		X	X	X
OPS.1.1.6.A13		X								X				
OPS.1.1.6.A14		X	X	X	X	X				X		X	X	X



OPS.1.2.2: Archiving

Description

Introduction

Archiving plays a special role within the document management process: on the one hand, documents are expected to be available until the expiry of a specified retention period. On the other hand, their confidentiality and integrity must be maintained. In addition, the context must be maintained so that the respective stored sequence can be reconstructed.

For the entire duration of long-term storage, corresponding safeguards for information maintenance and, if required, measures for maintaining evidence must be implemented.

The term "electronic archiving" is sometimes used synonymously with the term "electronic long-term storage" when referring to an IT context in German. For better clarity, the terms "archiving" or "digital long-term archive" are used in this module. An IT process for storing electronic documents is referred to as an "archive system", a "digital archive" or "long-term storage". The retention period of the documents depends on the statutory and other regulations, as well as the purpose of the data.

The term "documents" as used in this module includes data and documents unless these are expressly used with a differing meaning.

From a German legal perspective, the term "archiving" is substantiated and documented by the federal and state archiving laws. Hence, it must be differentiated from storage over a limited period of time, which is covered in this document. In a legally correct sense, "archiving" solely concerns government documents and refers to how the documents of a public authority are to be sorted and kept by the federal institution responsible (the Federal Archives) for an unlimited period of time as soon as they are no longer needed for the purposes of that public authority (see Sections 1 and 2 of the Federal Archives Act [BArchG]).

Objective

This module describes how documents can be securely archived for the long term such that they are reproducible and cannot be changed. To this end, it defines requirements that can be used to securely plan, implement and operate an archive system.

Not in Scope

The module on archiving describes security safeguards for storing and maintaining electronic documents for long-term storage within the framework of applicable retention periods. Safeguards for operative backups are not addressed in this module. Requirements in this regard are covered in CON.3 *Backup Concept*.

Digital long-term storage consists of individual components, including a database. The question of how such components can be operated in a secure and detailed manner is also not covered in the present module. Here, it is possible to build on the requirements from the modules APP.4.3 *Relational Database Systems*, SYS.1.1 *General Server* and SYS.1.8 *Storage Solutions*, for example.

Threat Landscape

For module OPS.1.2.2 *Archiving*, the following specific threats and vulnerabilities are of particular importance:

Inadequate Migration of Archive Systems

Archived data should typically remain stored over a very long period of time. During this period, the underlying technical system components, storage media and data formats may age physically or technically and become useless. Furthermore, compatibility issues regarding the data formats used may arise over the course of time.

If there is no reaction to the ageing of the existing system, it must be taken into account in the long term that it may no longer be physically possible to read raw archived data from the archiving media, for example, or that archived data may be changed due to physical errors in archive systems and archiving media.

Inadequate Indexing Keys for Archives

Electronic archives may contain very large amounts of data. In such cases, the individual datasets are stored in accordance with certain indexing keys, which is where a distinction must be made between business application index data and archiving system index data. If inappropriate indexing keys are being used, it may take a great deal of time to search through archived documents (if this is possible at all) or be impossible to clearly determine the semantics of the documents. There is also the risk that the inappropriate or limited selection of indexing keys will result in retention objectives not being met (e.g. the ability to provide proof to third parties).

Inadequate Documentation of Archive Access

Unauthorised archive access is normally discovered with the help of log files. However, if logging was not performed to the required extent, there is the risk that such access attempts will not be detected. As a consequence, attackers might obtain the information stored there without this being noticed and copy or change the information, for example.

Inadequate Transfer of Paper Data to an Electronic Archive

When scanning documents, the appearance or semantics of the data recorded may be compromised, or documents may even be lost. This may result in incorrect interpretations and calculations, such as if important parts of the document or the document stack are forgotten during the scan.

Insufficient Renewal of Cryptographic Procedures During Archiving

Cryptographic procedures used for signatures, seals, time stamps, technical evidence records or encryptions, for example, must be regularly adapted to the current state of the art to maintain their protective effect. If this is not done, the integrity of the document may be called into

question – for example, due to an outdated and insecure signature – which could mean the file is inadmissible as evidence in court. The confidentiality of an encrypted document can also be lost this way.

Insufficient Auditing of Archiving Procedures

If the archiving process is audited too infrequently or inaccurately, this may directly result in the entire process no longer working properly. The integrity of the archived documents themselves may thus be called into question. This may result in legal and economic disadvantages for the organisation: a file might not be admissible as evidence in court, for example, because it cannot be ruled out that the file has been manipulated.

Violation of Legal Framework Conditions Regarding the Use of Archive Systems

When archiving electronic documents, different legal framework conditions must be observed. If these are not met, this may have civil or criminal consequences (e.g. in cases involving minimum retention periods for tax, budgetary or other reasons).

Requirements

The specific requirements of module OPS.1.2.2 *Archiving* are listed below. As a matter of principle, the Archive Administrator is responsible for compliance with the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Archive Administrator
Further Roles	Chief Information Security Officer (CISO), IT Operation Department, User, Head of IT

Basic Requirements

For module OPS.1.2.2 *Archiving*, the following requirements **MUST** be implemented as a matter of priority:

OPS.1.2.2.A1 Determination of Influencing Factors for Electronic Archiving [Chief Information Security Officer (CISO)]

Before methods and products for electronic archiving are chosen, the technical, legal and organisational influencing factors **MUST** be determined and documented. The results **MUST** be incorporated into the archiving concept.

OPS.1.2.2.A2 Drawing Up an Archiving Concept [Chief Information Security Officer (CISO)]

It **MUST** be defined which aims are to be achieved by archiving. In particular, this **MUST** take into consideration which rules have to be followed, which employees are responsible and what the desired scope of functions and services is.

The results **MUST** be documented in an archiving concept. The management **MUST** be involved in this process. The archiving concept **MUST** be adapted to the current circumstances at regular intervals.

OPS.1.2.2.A3 Appropriate Installation of Archive Systems and Storage of Archive Media [Head of IT, IT Operation Department]

Since archive systems store an organisation's sensitive data in a central location, their IT components **MUST** be installed in secured rooms. It **MUST** be ensured that only authorised persons may access the rooms. In order to ensure that archive storage media can be stored over long periods of time, they **MUST** be stored appropriately.

OPS.1.2.2.A4 Consistent Indexing of Data During Archiving [Head of IT, IT Operation Department, User]

All data, documents and datasets stored in an archive **MUST** be indexed unambiguously in order to be able to find them during future queries. To this end, the desired structure and extent of an archive's index information **MUST** already be defined in the design phase.

OPS.1.2.2.A5 Regular Regeneration of Archived Data [Head of IT]

It **MUST** be ensured over the entire archiving period that

- the data format used can be processed by the applications used
- the data stored can be read and reproduced in the future in such a way that semantics and significance can be maintained
- the file system used on the storage medium can be processed by all components involved
- the storage media can be read at any time without technical issues
- the cryptographic methods used for encryption and the preservation of legal relevance by means of digital signatures, seals, time stamps or technical evidence records correspond to the state of the art

OPS.1.2.2.A6 Protection of the Integrity of the Index Database of Archive Systems [Head of IT, IT Operation Department]

The integrity of the index database **MUST** be safeguarded and verifiable. In addition, the index database **MUST** be backed up regularly. It **MUST** be possible to restore the backups. Medium-sized and large archives **MUST** have redundant index databases.

OPS.1.2.2.A7 Regular Backups of System and Archive Data [Head of IT, IT Operation Department]

All archive data, the related index databases, and the system data **MUST** be backed up at regular intervals (see *CON.3 Backup Concept*).

OPS.1.2.2.A8 Logging of Archive Access [Head of IT, IT Operation Department]

All attempts to access electronic archives **MUST** be logged. To this end, dates, times, users, client systems and the actions performed (as well as any error messages) **SHOULD** be recorded. The retention period of the log data **SHOULD** be defined in the archiving concept.

The log data for archive access SHOULD be evaluated regularly. In so doing, the internal specifications of the organisation SHOULD be taken into account.

The events (e.g. system errors, timeouts, or copy datasets) that are to be displayed to specific employees SHOULD also be defined. Critical events SHOULD be evaluated and, if required, escalated further immediately upon coming to light.

OPS.1.2.2.A9 Selection of Suitable Data Formats for Archiving Documents [Head of IT, IT Operation Department]

A suitable data format MUST be selected for archiving. It MUST ensure that archived data and selected features of the initial document medium can be reproduced in the long term in a format that is true to the original.

It MUST be possible to unambiguously interpret and electronically process the document structure of the selected data format. The syntax and semantics of the data formats used SHOULD be documented and published by a standardisation organisation. A loss-free image compression method SHOULD be used for evidence and audit-compliant archiving.

Standard Requirements

For module OPS.1.2.2 *Archiving*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

OPS.1.2.2.A10 Drawing Up a Policy for Using Archive Systems [Head of IT, IT Operation Department]

It SHOULD be ensured that employees use the archive system as prescribed in the archiving concept. To this end, an administration and user policy SHOULD be drawn up. The administration policy SHOULD cover the following items:

- specification of the responsibility for operation and administration
- agreements regarding the performance parameters during operation (service level agreements)
- terms regarding the assignment of site and data access rights
- terms regarding the assignment of access rights to the services provided by the archive
- regulations regarding the handling of archived data and archive media
- monitoring of the archive system and the environmental conditions
- rules on backups
- rules on logging
- separation of producers and consumers (OAIS model)

OPS.1.2.2.A11 Instruction Regarding the Administration and Operation of the Archive System [Head of IT, IT Operation Department, User]

The IT Operation Departments and the users responsible SHOULD be trained in their field of responsibility.

The IT Operation Departments' training SHOULD cover the following subjects:

- system architecture and security mechanisms of the archive system used and the underlying operating system
- installation and operation of the archive system and handling of archive media
- documentation of the administrative activities
- escalation procedures

The user training SHOULD cover the following subjects:

- handling the archive system
- operating the archive system
- legal framework conditions of archiving

Performance of and participation in the training measures SHOULD be documented.

OPS.1.2.2.A12 Monitoring the Storage Resources of Archive Media [Head of IT, IT Operation Department]

The capacity available in the archive media MUST be monitored continuously. Once it has fallen below a defined threshold, a responsible employee MUST be alarmed automatically. It SHOULD be ensured that alarming takes place in a role-based manner. A sufficient number of empty archive media MUST be available at any point in time to quickly prevent storage bottlenecks.

OPS.1.2.2.A13 Regular Auditing of the Archiving Processes

It SHOULD be checked regularly whether the archiving processes are still working correctly and properly. A checklist SHOULD be drawn up for this that includes questions about responsibilities, organisational processes, use of archiving, redundancy of the archived data, administration and technical assessment of the archive system. The audit results SHOULD be documented transparently and compared against the target condition. Deviations SHOULD be investigated.

OPS.1.2.2.A14 Regular Observation of the Market for Archive Systems [Head of IT]

The market for archive systems SHOULD be observed regularly and systematically. Among other things, the following criteria SHOULD be taken into account: changes in standards, technology changes among manufacturers of hardware and software, published security gaps or vulnerabilities and cryptographic algorithms that are no longer suitable.

OPS.1.2.2.A15 Regular Processing of Cryptographically Secured Data During Archiving [Head of IT, IT Operation Department]

Developments in the field of cryptography should be continuously monitored to assess the on-going reliability and security of a given algorithm (see also OPS.1.2.2.A20 *Appropriate Use of Cryptographic Procedures*)

Archive data that has been secured with cryptographic procedures that will no longer be suitably secure in the foreseeable future SHOULD be re-secured in good time with secure procedures (e.g. encryption or signing).

OPS.1.2.2.A16 Regular Renewal of Technical Archive System Components [Head of IT, IT Operation Department]

Archive systems SHOULD comply with the current state of the art over long periods of time. New hardware and software SHOULD be tested comprehensively before being installed in a running archive system. When commissioning new components or introducing new file formats, a migration concept SHOULD be drawn up. This concept SHOULD describe all changes, tests, and expected test results. Conversion of the individual data SHOULD be documented (using a transfer note).

When converting archive data to new formats, it SHOULD be checked whether the data must also be archived in its initial format as a consequence of legal requirements.

OPS.1.2.2.A17 Selection of an Appropriate Archive System [Head of IT]

A new archive system SHOULD always be selected on the basis of the specifications mentioned in the archiving concept. It SHOULD meet the requirements formulated therein.

OPS.1.2.2.A18 Use of Appropriate Archive Media [Head of IT, IT Operation Department]

Appropriate media SHOULD be selected and used for archiving. In so doing, the following aspects SHOULD be taken into consideration: the data volume to be archived, mean access times, and mean simultaneous users accessing the archive system. The archive media SHOULD also meet the requirements regarding long-term archiving with regard to audit compliance and useful life.

OPS.1.2.2.A19 Regular Function and Recovery Tests for Archiving [Head of IT, IT Operation Department]

Regular function and recovery tests SHOULD be performed for archiving. The archive storage media SHOULD be checked at least once a year as to whether they are still readable and their integrity remains intact. Appropriate processes SHOULD be defined for troubleshooting.

Furthermore, the hardware components of the archive system SHOULD be checked for sound functionality at regular intervals. It SHOULD be checked regularly whether all archiving processes work without any errors.

Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.2.2 *Archiving* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.1.2.2.A20 Appropriate Use of Cryptographic Procedures During Archiving [Head of IT] (CI)

In order to cover long retention periods, archive data SHOULD only be secured with cryptographic procedures that are based on current standards.

OPS.1.2.2.A21 Transfer of Paper Data to Electronic Archives (CI)

If documents on paper and visual objects are digitalised and transferred to an electronic archive, it SHOULD be ensured that the digital copy matches the original document in terms of its images and content.

Additional Information

For more information about threats and security safeguards for module OPS.1.2.2 *Archiving*, see the following publications, among others:

[AlgKat]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung: Auflistung geeigneter Algorithmen und Parameter [Announcement Regarding the Electronic Signature pursuant to the Signature Act and the Signature Ordinance: Overview of Suitable Algorithms], Federal Network Agency (BnetzA), 2017, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/2016Algorithmenkatalog.pdf?__blob=publicationFile&v=1 , last accessed on 26.07.2018
[DIN31644]	DIN 31644:2012-04: Information and documentation - Criteria for trustworthy digital archives, April 2012
[DIN31647]	DIN 31647:2015-05: Information and documentation - Preservation of evidence of cryptographically signed documents, May 2015
[EIDAS-DG]	EIDAS-DG: Gesetz zur Durchführung der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-Durchführungsgesetz), [Draft Act implementing Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Implementing Act)], Federal Gazette 2017 Part I No. 52, issued at Bonn on 28 July 2017
[EIDAS-VO]	EIDAS-VO: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC
[RESISCAN]	BSI TR-03138 RESISCAN: Replacement Scanning, March 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03138/TR-03138.pdf?__blob=publicationFile&v=4 , last accessed on 26.07.2018
[RFC4998]	Evidence Record Syntax (ERS): RFC4998, August 2007, https://tools.ietf.org/html/rfc4998 , last accessed on 26.07.2018

[RFC6283]	Extensible Markup Language Evidence Record Syntax (XMLERS): RFC 6283, July 2011, https://www.ietf.org/rfc/rfc6283.txt , last accessed on 26.07.2018
[SOG-IS]	SOG-IS Crypto Working Group: SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms, 2016, https://www.sogis.org/uk/supporting_doc_en.html , last accessed on 26.07.2018
[TR-ESOR]	BSI TR- 03125 TR-ESOR: Preservation of Evidence of Cryptographically Signed Documents, 2014, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html , last accessed on 26.07.2018
[TR-ESOR-B]	BSI TR-03125 TR-ESOR: Preservation of Evidence of Cryptographically Signed Document, Annex TR-ESOR-B: German Federal Agency Profiling, January 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_B_V1_2_1.pdf?__blob=publicationFile&v=2 , last accessed on 26.07.2018
[TR-ESOR-E]	BSI TR-03125 TR-ESOR: Preservation of Evidence of Cryptographically Signed Documents, Annex TR-ESOR-E: Concretisation of the Interfaces on the Basis of the eCard-API-Framework, 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_E_V1_2_1.pdf?__blob=publicationFile&v=2 , last accessed on 26.07.2018
[TR-ESOR-F]	BSI TR-03125 TR-ESOR: Preservation of Evidence of Cryptographically Signed Documents, Annex TR-ESOR-F: Formats, 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_F_V1_2_1.pdf?__blob=publicationFile&v=2 , last accessed on 26.07.2018
[TR-ESOR-M3]	BSI-TR-03125 TR-ESOR: Preservation of Evidence of Cryptographically Signed Documents ,Annex TR-ESOR-M.3: ArchiSig-Module, 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_M3_V1_2_1.pdf?__blob=publicationFile&v=2 , last accessed on 26.07.2018
[TR-ESOR-XB]	BSI TR-03125 TR_ESOR: BSI Technical Guideline 03125 Preservation of Evidence of Cryptographically Signed Documents, Annex TR-ESOR-Profile-XBDP: XAIP Profiling with XBARCH, XDOMEA and PREMIS, 2014, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_XBDP_V1_2_1.pdf?__blob=publicationFile&v=2 , last accessed on 26.07.2018
[TS119132]	ETSI: Electronic Signatures and Infrastructures (ESI): Cryptographic Suites, Version 1.2.1, May 2015
[VDG]	Trust Services Act - VDG: Article 1 of the Act Implementing Regulation (EU) No 910/2014 of the European Parliament and the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (eIDAS Implementing Act), Federal Gazette 2017 Part I

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.1.2.2 *Archiving*:

- G 0.2 Unfavourable Climatic Conditions
- G 0.4 Pollution, Dust, Corrosion
- G 0.14 Interception of Information / Espionage
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.22 Manipulation of Information
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.37 Repudiation of Actions
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.2	G 0.4	G 0.14	G 0.18	G 0.19	G 0.22	G 0.25	G 0.26	G 0.28	G 0.29	G 0.30	G 0.31	G 0.37	G 0.45	G 0.46
OPS.1.2.2.A1				X						X			X		
OPS.1.2.2.A2				X							X				
OPS.1.2.2.A3	X	X													
OPS.1.2.2.A4				X			X	X							
OPS.1.2.2.A5				X						X					
OPS.1.2.2.A6							X	X	X						X
OPS.1.2.2.A7														X	X
OPS.1.2.2.A8			X			X				X					
OPS.1.2.2.A9														X	X
OPS.1.2.2.A10				X						X		X			
OPS.1.2.2.A11							X	X			X	X			
OPS.1.2.2.A12							X	X						X	X
OPS.1.2.2.A13				X						X					
OPS.1.2.2.A14				X			X	X	X						
OPS.1.2.2.A15				X			X	X	X						X
OPS.1.2.2.A16				X											X
OPS.1.2.2.A17							X	X							
OPS.1.2.2.A18				X					X	X					
OPS.1.2.2.A19				X			X	X							
OPS.1.2.2.A20							X	X	X					X	X
OPS.1.2.2.A21			X		X					X			X		



OPS.1.2.3: Exchange of Information and Storage Media

Description

Introduction

This module covers the secure exchange of information. The focus is on digital and analogue storage media as transport media, as well as on the exchange of information during face-to-face meetings or via IT networks. Even when a broadband network connection is available, it can be sensible or necessary to send storage media to exchange information. One possible reason involves a lack of a sufficiently trustworthy connection (or none at all) between the corresponding IT systems. Storage media can be exchanged in person or by conventional post.

Objective

The objective of this module is to secure the exchange of information between various communication partners and IT systems. In particular, it outlines the aspects that should be kept in mind to adequately protect data when exchanging storage media.

Not in Scope

This module should always be used if information is exchanged with offices outside the organisation itself or its premises and the internal network cannot be used. In particular, it should be used if

- new transportation paths are established (new communication partners, new media, new networks) or
- information is exchanged with the help of storage media. In addition to transmission, the storage and handling of storage media should be given special attention.

The protection of network connections is dealt with in other modules of the IT-Grundschutz Compendium. Subsequent processing in the target IT system is also not considered. In this module, the focus is on the fundamental rules for a secure exchange of information, particularly with the use of mobile storage media. The reasons why no network exists between the corresponding IT systems or the network available is not trustworthy enough are not considered.

This module also covers the storage of data in the sending and receiving systems when this directly relates to the exchange of storage media and describes how to handle the storage media before and after transfer. This module covers mobile storage media such as removable disks, optical storage media, USB pen drives and hard disks in addition to paper documents.

Threat Landscape

For module OPS.1.2.3 *Exchange of Information and Storage Media*, the following specific threats and vulnerabilities are of particular importance:

Defective Storage Media

Damage, errors or failures can occur with all types of storage media. This can become a problem when the information stored on the storage media is not saved anywhere else and cannot be reconstructed quickly and easily.

Inadmissible Temperature and Humidity

Extreme temperatures and humidity can affect the proper functioning of storage media. For any type of storage media, there are defined limits within which proper functioning is guaranteed. If the corresponding values are too low or too high, this can result in operational disruptions and equipment failures. Excessive fluctuations in temperature or excessive humidity can cause data errors on digital storage media.

Improperly Packed Storage Media

Storage media are subjected to particular strain during transportation or shipping. With storage media, even slight contamination can lead to data errors. Hard disks can be destroyed when the read/write head crashes, and tapes and cartridges can be damaged by direct mechanical impact. CD-ROMs and DVDs can be rendered useless by surface scratches.

Data Loss Due to Strong Magnetic Fields

Typical storage media that use a magnetic storage medium include removable disks, cartridges and tapes. These storage media are sensitive to interference from magnetic fields and should not be brought near such sources of radiation.

Delayed Availability of Storage Media

When exchanging storage media, it is of particular importance to many business processes that the media reach their recipients on time and can quickly be put to use. Even small errors in labelling can result in storage media not reaching their destination by the required time. If the necessary interfaces or equipment are not available locally, it may not be possible to read storage media under some circumstances. The resultant delays can cause significant damage.

Uncontrolled Delivery of Information or Storage Media

If information or storage media are forwarded without controls or delivered incorrectly, there is a risk that confidential data may fall into the hands of unauthorised parties or fail to reach the correct destination on time.

Inadequate Key Management for Encryption

If encryption systems are used to protect the confidentiality of data to be transmitted, the desired protection can be undermined by inadequate key management. For example, a key that is easy to guess can be chosen or the cryptographic key used for encryption and decryption can be sent to the communication partner by insecure means. In the simplest negative example, encrypted information and the corresponding encryption key are sent using the same storage

medium. In this case, anyone who gains possession of the storage medium can decrypt the information, assuming this person knows which encryption method was used.

Loss of Storage Media During Transport

If storage media are sent using packaging that is not particularly sturdy (mailing envelopes or other such packaging), there is a risk that the storage media will be lost if the packaging is damaged. There is also a risk of losing the package after it has been received, while it is in the post or due to carelessness on the part of the delivery service. Storage media are becoming ever smaller, which makes it easier for them to be lost in transport.

If the information on the storage media is not encrypted, the data may also fall into the wrong hands if the delivery is lost.

Sharing of False or Internal Information

When information is shared, it is not uncommon for additional information to be inadvertently disclosed along with what was intended. Confidential information or information not intended for the public falls into the wrong hands in this manner on a regular basis. Storage media are sometimes passed on without deleting the data previously stored on them using a suitable deletion method. Confidential documents can also be accidentally sent to the wrong recipients, or letters containing internal comments can be printed out and posted.

Theft, Manipulation or Destruction of Storage Media

Both external and internal attackers may try to steal, manipulate or destroy storage media for various reasons (espionage, revenge, ill will, frustration). Potential manipulations range from the unauthorised viewing of sensitive data and modification of the content of data to the destruction of storage media.

Malware in Transmitted Files or on Storage Media

If the working environment is not sufficiently secured against malware, storage media containing malware may be passed on to external parties. The stored data can be destroyed or adulterated as a result, but worst of all, IT systems on the recipient side can be compromised. However, the reputational and financial damage that can result from malicious software can also be significant.

Unauthorised Copying of Information or Storage Media

If information or storage media are exchanged or transported via an insecure transportation route, there is a risk that the information transmitted may be copied by unauthorised parties during transportation. Attackers can also attempt to eavesdrop on communications over IT networks.

Requirements

The specific requirements of module OPS.1.2.3 *Exchange of Information and Storage Media* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	IT Operation Department, Head of Organisation, Postal Department, User, Process Owner

Basic Requirements

For module OPS.1.2.3 *Exchange of Information and Storage Media*, the following requirements MUST be implemented as a matter of priority:

OPS.1.2.3.A1 Determination of Admissible Communication Partners [Head of Organisation]

Within the organisation, it MUST be determined which communication partners may receive and pass on which information. This MUST be communicated for all operational purposes in the organisation. Before exchanging information, employees MUST clarify whether the recipient has the necessary authorisations to receive and subsequently process the information.

OPS.1.2.3.A2 Regulations Concerning Exchanges of Information [Head of Organisation]

Before information is exchanged, there MUST be a clarification regarding the extent to which the relevant information requires protection, with whom the information may be exchanged and how, in concrete terms, it should be protected in the process. The employees MUST be made sufficiently aware of this requirement. The recipients MUST be made aware of the fact that the data transferred may only be used for the purpose for which it was passed on.

OPS.1.2.3.A3 Instruction of Personnel on Exchanges of Information [Process Owner]

The personnel MUST be informed of the framework conditions that apply to exchanges of information. They MUST know what information they can pass on, as well as when, where and how.

OPS.1.2.3.A4 Protection Against Malware [User]

Digital data MUST be checked for malware both in advance by the sender and by the recipient. The virus protection programs used must be up to date.

OPS.1.2.3.A5 Reporting Losses [User]

Employees MUST immediately report the loss or theft of a storage medium or any suspicion of manipulation during the exchange of data. There SHOULD be clear reporting channels and contact persons in every organisation for this purpose.

Standard Requirements

For module OPS.1.2.3 *Exchange of Information and Storage Media*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

OPS.1.2.3.A6 Agreements on Exchanging Information with External Parties [Head of Organisation]

If information is exchanged regularly with external partners, the framework conditions for this SHOULD be formally agreed.

OPS.1.2.3.A7 Regulations Concerning Exchanges of Storage Media [Head of Organisation]

The proper exchange of storage media SHOULD be controlled. Protection of the storage media within the organisation itself, during transport and on the recipient side SHOULD be defined. The type of storage media and the protection needs of the information SHOULD be considered when selecting the mode of transport. Furthermore, it SHOULD be specified when and how storage media are to be physically deleted.

OPS.1.2.3.A8 Physical Deletion of Storage Media Before and After Usage [User]

Before and after an exchange of data, storage media which are used for other purposes SHOULD be deleted physically. Employees SHOULD be provided with suitable programs for physical deletion.

OPS.1.2.3.A9 Removal of Residual Information from Files Prior to Sharing [User]

The users SHOULD be informed of the dangers of residual and additional information in files. The users SHOULD be taught how residual and additional information in files can be avoided. Residual information SHOULD be removed accordingly. Random checks for any residual information contained therein SHOULD be carried out before files are passed on.

OPS.1.2.3.A10 Conclusion of Non-Disclosure Agreements [Head of Organisation]

Non-disclosure agreements SHOULD be concluded with external employees before they are granted access to confidential information. The non-disclosure agreements used SHOULD take all important aspects relating to the protection of confidential information into account.

OPS.1.2.3.A11 Compatibility Checks on Sender and Recipient Systems [IT Operation Department]

Before information is exchanged, the systems and products used SHOULD be checked for compatibility on the sender and recipient sides.

OPS.1.2.3.A12 Appropriate Labelling of Storage Media for Shipping [User]

When labelling storage media, care SHOULD be taken to ensure that the sender and recipient are immediately identifiable. The labels on storage media or their packaging SHOULD enable the recipient to clearly identify the contents of the storage media. The labelling of storage media containing sensitive information SHOULD ensure that NO conclusions can be drawn regarding the type or contents of the information.

Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.1.2.3 *Exchange of Information and Storage Media* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.1.2.3.A13 Encryption and Digital Signatures [User] (CI)

Confidential information SHOULD be encrypted before it is exchanged. Information with high integrity requirements SHOULD be digitally signed. Suitable crypto methods which meet the protection needs and can be used without any problems on the sender and recipient sides SHOULD be selected for this. Appropriate key management SHOULD be established for the use of cryptographic methods.

OPS.1.2.3.A14 Storage Media Management [Head of Organisation, IT Operation Department] (CIA)

For higher protection needs, a storage media management system SHOULD be established in order to regulate access to storage media, their labelling and their proper storage. There SHOULD be rules on proper handling, including the storage, transfer, transport and deletion of all types of storage media. An inventory list SHOULD be drawn up. The storage media SHOULD be handled properly in accordance with the manufacturer specifications.

OPS.1.2.3.A15 Secure Shipping Methods and Packaging [Postal Department, User] (C)

When information is subject to higher protection needs, it SHOULD be determined how it can be appropriately protected during exchanges. Secure packaging SHOULD be used to ship storage media so that any manipulation will result in apparent changes to the packaging. The sender SHOULD inform the Postal Department of the types of shipping and packaging that are required. As a rule, the data SHOULD be encrypted.

OPS.1.2.3.A16 Safekeeping of Storage Media Before and After Shipping [User, Postal Department] (CIA)

Storage media with written data SHOULD be stored in a safe place that can only be accessed by authorised users. All employees involved SHOULD be instructed to ensure the proper and secure storage and handling of storage media.

OPS.1.2.3.A17 Verification of Storage Media Before Shipping [User] (CI)

Before storage media are sent, the following SHOULD be checked:

- whether the desired information is contained in full, and
- that the media contain no additional information which should not be passed on.

OPS.1.2.3.A18 Backup Copies of Transferred Data [User] (A)

If the data to be transferred has only been created or collected specifically for transfer and is not stored on any other data medium, a backup copy of this data SHOULD be made. If the data is lost or damaged in transit, it can then be sent again quickly and easily.

Additional Information

For more information about threats and security safeguards for module OPS.1.2.3 *Exchange of Information and Storage Media*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[NIST800150]	Guide to Cyber Threat Information Sharing: Special Publication 800-150, October 2016, http://dx.doi.org/10.6028/NIST.SP.800-150 , last accessed on 05.10.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.1.2.3 *Exchange of Information and Storage Media*:

- G 0.2 Unfavourable Climatic Conditions
- G 0.4 Pollution, Dust, Corrosion
- G 0.14 Interception of Information / Espionage
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.17 Loss of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.22 Manipulation of Information
- G 0.24 Destruction of Devices or Storage Media
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.29 Violation of Laws or Regulations
- G 0.38 Misuse of Personal Information
- G 0.39 Malware
- G 0.42 Social Engineering
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.2	G 0.4	G 0.1 4	G 0.1 6	G 0.1 7	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 2	G 0.2 4	G 0.2 5	G 0.2 6	G 0.2 9	G 0.3 8	G 0.3 9	G 0.4 2	G 0.4 5	G 0.4 6
OPS.1.2.3.A1							X	X	X				X	X		X		
OPS.1.2.3.A2			X				X	X					X	X		X		
OPS.1.2.3.A3			X				X						X	X	X	X	X	
OPS.1.2.3.A4												X			X		X	X
OPS.1.2.3.A5				X	X									X			X	
OPS.1.2.3.A6			X				X	X	X				X	X				
OPS.1.2.3.A7			X				X			X	X	X	X	X	X		X	
OPS.1.2.3.A8			X				X							X				
OPS.1.2.3.A9			X				X							X				
OPS.1.2.3.A10							X						X	X				
OPS.1.2.3.A11						X												
OPS.1.2.3.A12					X		X	X						X			X	
OPS.1.2.3.A13			X	X			X		X					X				X
OPS.1.2.3.A14										X	X	X					X	
OPS.1.2.3.A15	X	X	X	X			X			X	X	X		X				
OPS.1.2.3.A16	X	X	X	X			X							X				
OPS.1.2.3.A17							X							X				X

OPS.1.2.3.A1 8	X	X			X					X	X	X					X	
-------------------	---	---	--	--	---	--	--	--	--	---	---	---	--	--	--	--	---	--



OPS.1.2.4: Teleworking

Description

Introduction

Teleworking is understood to refer to all tasks that are performed completely outside of the business premises and buildings of the employer using information and communication technology. There are various forms of teleworking. For example, it can be home-based teleworking performed at the residence of the employee. It is also possible for the employees to work at the customer's or supplier's location within the framework of on-site teleworking using equipment supplied by their employer. Another teleworking method involves so-called telecentres, or branch or neighbourhood offices.

There are two basic types of home-based teleworking: teleworking in which the work is performed only at home and alternating teleworking. In alternating teleworking, the employee alternates between working from a home office and working at the workplace of their employer.

Objective

The objective of this module is to protect the information which is stored, processed and transmitted during teleworking. To this end, typical threats are presented and special requirements on teleworking are defined.

Not in Scope

This module focuses on the forms of teleworking performed exclusively or only in part from the home environment. It is assumed that a telecommunication link is available between the workstation for teleworking and the organisation to allow information to be exchanged and data accessed in the organisation as necessary. The requirements of this module cover three different areas:

- the organisation of teleworking
- the teleworking computer of the teleworker
- the communication link between the teleworking computer and the organisation

Security requirements for the infrastructure of the teleworking workplace are not included in the present module; they are described in module INF.8 *Working from Home*. The requirements of module INF.9 *Mobile Workplace* (which covers some of the same topics as this module) must be considered.

Threat Landscape

For module OPS.1.2.4 *Teleworking*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Rules for the Teleworking Workplace

Since a teleworking workplace is geographically located outside the organisation, it requires individually adapted organisational agreements. If such rules do not exist, employees may not know that they are required to perform backups on their own (for example). Sometimes, they also do not know how to handle security-relevant events at the teleworking workplace. For example, if confidential information falls into the wrong hands, unauthorised persons could use it to seriously disadvantage the organisation.

Non-Existent or Inadequate Training of Teleworkers

Teleworkers are more or less on their own when at their workplace. If a teleworker has not received adequate training on the handling of the corresponding IT, problems may result in longer downtime because it may (for example) be necessary for one of the organisation's IT support technicians to drive to the teleworking workplace in order to eliminate the problems.

Unauthorised Private Use of Teleworking Workstations

Using a teleworking computer for private purposes is easier at home because the employer has only limited usage monitoring capabilities. It is thus possible that untested and unapproved software will be used and that malware will infect the teleworking computer through careless use. This might result in confidential information becoming compromised, for example.

It is possible that the computer will be misused not only by the teleworker, but by family members or visitors, as well. Damage related to erased hard disks, for instance, may result in re-installation costs or the need to re-enter data.

Delays Caused by Temporarily Restricted Availability of Teleworkers

Normally, a teleworker does not have fixed working hours at the teleworking workplace. An agreement is only made regarding their required availability at certain times. In the case of alternating teleworking, the teleworker's working hours are divided between the teleworking workplace and the workplace at the organisation.

If information must be obtained from the teleworker or passed quickly to the teleworker on short notice, the teleworker's limited availability may result in delays. Even sending the information in an e-mail might not necessarily shorten the response time because it cannot be guaranteed that the teleworker will read the e-mail promptly.

Depending on the situation and organisation, delays caused by the temporarily restricted availability of teleworkers may have different effects and limit availability in a different way.

Poor Integration of Teleworkers into the Information Flow

Since teleworkers do not work in the organisation every day, they have fewer opportunities to participate in direct exchanges of information with supervisors and work colleagues. They may become cut off from what is happening in the organisation and, for example, identify less with the organisation as a result. Due to a lack of information, there may also be errors in work pro-

cesses and operational processes that limit the teleworker's productivity. If the flow of information to the teleworker is not ensured, important messages on the topic of information security may not reach the teleworker in good time.

Inadequate Regulations Concerning Teleworker Substitution

In general, the tasks of the teleworker must be designed such that they can work in a largely independent manner. It can thus be difficult to provide an appropriate substitute for the teleworker if they are on sick leave. In particular, it may be difficult to provide the substitute with the required documents or data stored on the teleworking computer if there is no way to access the home workplace of the teleworker.

Non-Compliance with Security Measures

Particularly at the teleworking workplace, a lack of monitoring capabilities may result in the employee failing to implement some or all of the recommended or required security safeguards. This can cause damage which otherwise could have been prevented, or at least minimised. Depending on the role of the employee in question and the importance of the safeguard ignored, the resulting damage could even be very serious (e.g. confidential information may fall into the wrong hands). Such information could be used to seriously disadvantage the organisation.

Requirements

The specific requirements of module OPS.1.2.4 *Teleworking* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Human Resource Department, IT Operation Department, Teleworker, Head of Organisation, Head of IT, Supervisor

Basic Requirements

For module OPS.1.2.4 *Teleworking*, the following requirements **MUST** be implemented as a matter of priority:

OPS.1.2.4.A1 Rules on Teleworking [Supervisor, Human Resource Department]

All the relevant aspects of teleworking **MUST** be specified. The applicable rules or a corresponding leaflet explaining the security safeguards to be considered **MUST** be provided to teleworkers. Contentious points **MUST** be clarified in employment agreements or separate agreements between the teleworker and employer as a supplement to their employment contract. A substitute **MUST** be named for each teleworker. Substitution arrangements **SHOULD** be practised regularly. The rules **MUST** be updated at regular intervals.

OPS.1.2.4.A2 Security-Related Requirements for Teleworking Computers [IT Operation Department, Head of IT]

All security-related requirements to be fulfilled by a teleworking computer **MUST** be specified. All site and data access capabilities on the communication computers of the organisation **MUST** be limited to the minimum necessary.

It **MUST** be ensured that only authorised persons are allowed to access the teleworking computers. Moreover, the teleworking computer **MUST** be protected so that it can be used only for the authorised purpose.

OPS.1.2.4.A3 Security-Related Requirements for Communication Links [IT Operation Department, Head of IT, Teleworker]

Security-related requirements for the communication link between the teleworking computer and the organisation **MUST** be defined. Here, it **MUST** be ensured that the confidentiality, integrity and authenticity of the transmitted data are guaranteed.

Any employed communication protocols and security mechanisms **MUST** meet the defined requirements of the organisation. The strength of the security mechanisms required for this purpose **SHOULD** depend on the protection needs of the data transmitted. In addition, the authenticity of the communication partner **MUST** be guaranteed.

OPS.1.2.4.A4 Backups During Teleworking [IT Operation Department, Teleworker]

All data processed while teleworking **MUST** be backed up in a timely manner. To this end, backups **MUST** be performed either locally on external storage media or centrally via the link to the organisation's network.

The backup procedure selected **MUST** be adequate and suitable for handling the volumes of data to be backed up. The teleworkers **MUST** perform as few tasks as possible themselves when backing up data to ensure a problem-free process. One generation of the backup storage media **SHOULD** be stored at the organisation.

OPS.1.2.4.A5 Awareness and Training of Teleworkers [Supervisor, Head of IT]

A leaflet **MUST** be issued to make the teleworkers aware of the risks connected to teleworking. Furthermore, they **MUST** be instructed on the corresponding security safeguards of the organisation and trained on how to deal with them. The training and awareness-raising measures for teleworkers **SHOULD** be repeated at regular intervals.

Standard Requirements

For module OPS.1.2.4 *Teleworking*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

OPS.1.2.4.A6 Creating a Security Concept for Teleworking [Supervisor, Head of IT, Head of Organisation]

A security concept for teleworking that describes the security objectives, protection needs, security requirements and risks involved **SHOULD** be drawn up. The concept **SHOULD** be reviewed and updated regularly. The security concept for teleworking **SHOULD** be coordinated with the overall security concept of the organisation.

OPS.1.2.4.A7 Regulated Use of Teleworking Communication Capabilities [IT Operation Department, Teleworker]

Clear rules SHOULD be specified regarding which communication capabilities may be used under which general framework conditions for the purpose of teleworking. There SHOULD be rules regarding the professional and private use of Internet services when teleworking. Here, it SHOULD also be clarified whether private use is generally allowed or prevented.

OPS.1.2.4.A8 Flow of Information Between the Teleworker and the Institution [Supervisor, Teleworker]

Regular intra-company exchanges of information between teleworkers, colleagues and the organisation SHOULD be ensured. All teleworkers SHOULD receive information on changed security requirements and other security-relevant aspects in a timely manner. All colleagues of the corresponding teleworker SHOULD know when and where they can be contacted. Technical and organisational teleworking rules on the performance of tasks, security incidents and other problems SHOULD be specified and communicated to the teleworker.

OPS.1.2.4.A9 Support and Maintenance Concept for Teleworking Workplaces [IT Operation Department, Head of IT, Teleworker]

A special support and maintenance concept SHOULD be drawn up for teleworking workplaces. This concept SHOULD specify the following aspects: contact persons for user services, maintenance dates, remote maintenance, transport of IT devices, and the introduction of standard teleworking computers. Contact persons for hardware and software problems SHOULD be named to help ensure that the teleworkers can continue to work.

OPS.1.2.4.A10 Analysis of Teleworking Workplace Requirements [IT Operation Department, Head of IT]

A requirements analysis SHOULD be performed before setting up a teleworking workplace. It SHOULD include the hardware and software components required for the teleworking workplace. The requirements for the relevant teleworking workplace SHOULD be agreed with the persons in charge of IT. The protection needs of the information processed at the teleworking workplace SHOULD always be determined and documented.

Requirements in Case of Increased Protection Needs

For module OPS.1.2.4 *Teleworking* there are no Requirements in Case of Increased Protection Needs.

Additional Information

For more information about threats and security safeguards for module OPS.1.2.4 *Teleworking*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018

[NIST80046]	Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security: NIST Special Publication 800-46, Revision 2, July 2016, http://dx.doi.org/10.6028/NIST.SP.800-46r2 , last accessed on 05.10.2018
-------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.1.2.4 *Teleworking*:

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.40 Denial of Service

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.14	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.24	G 0.25	G 0.30	G 0.31	G 0.32	G 0.33	G 0.40	G 0.45	G 0.46
OPS.1.2.4.A1	X	X	X	X	X	X			X	X	X	X		X	X
OPS.1.2.4.A2	X		X	X	X	X			X	X			X	X	X
OPS.1.2.4.A3	X		X	X	X	X			X	X			X		X
OPS.1.2.4.A4	X			X	X	X	X		X		X		X	X	X
OPS.1.2.4.A5	X	X	X	X	X	X									X
OPS.1.2.4.A6		X					X	X				X		X	
OPS.1.2.4.A7	X	X	X	X	X	X			X	X	X				X
OPS.1.2.4.A8		X										X			X
OPS.1.2.4.A9		X						X							X
OPS.1.2.4.A10		X													



OPS.2.1: Outsourcing for Customers

Description

Introduction

Within the framework of outsourcing, organisations (outsourcing customers) outsource business processes and services (e.g. security or cleaning personnel) entirely or partially to external service providers (outsourcing service providers). Operation of hardware and software may also be outsourced as a service. Regardless of what is being outsourced, every outsourcing process requires a strong commitment to the external service provider and the quality and quantity of its services. Especially for customers, this relationship is associated not only with opportunities, but also with significant risks (e.g. strong dependencies, loss of proprietary knowledge, and loss of monitoring and control options). Hence, information security aspects must be taken into consideration appropriately during the entire lifecycle of an outsourcing process.

The focus of this module consists of requirements that outsourcing customers should consider and implement within the framework of every phase of an outsourcing project.

Objective

The objective of this module is to ensure that all security objectives of the outsourcing customer are still being complied with after business processes or services are handed over to an outsourcing service provider and that the agreed security level is constantly maintained (and improved). Outsourcing must not result in any uncontrollable risks for the outsourcing organisation regarding information security.

Not in Scope

This module includes threats and security requirements from the outsourcing customers' point of view and is limited exclusively to the requirements regarding the protection of information on the part of the outsourcing organisation.

Transmission paths to outsourcing service providers cannot be secured by implementing these requirements.

The terms "outsourcing" and "cloud" have many parallels. For outsourcing customers, requirements regarding the use of cloud services must normally be taken into consideration as well.

Threat Landscape

For module OPS.2.1 *Outsourcing for Customers*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Rules Regarding Information Security

Within the framework of an outsourcing project, large amounts of information are typically transmitted between the customer and the outsourcing service provider. Depending on the protection needs of the information to be processed, non-existent or insufficient rules may result in damage. For example, this is the case if the rules and instructions for managing the service provider are not updated in the event of technical, organisational or personnel changes (e.g. when new contact persons take over). The possible shortcomings in rules here ranges from ambiguities in responsibilities and control functions to rules that are incomprehensible, incoherently formulated or simply not in place.

Incorrect Administration of Site, System and Data Access Rights

Depending on the outsourcing project, the outsourcing service provider's employees may require site, system and data access rights for IT systems, information, buildings or rooms on the customer side. If the processes of granting, managing and controlling these rights are characterised by poor rules and rights are thus assigned in an unauthorised manner in extreme cases, the necessary protection needs of the information of the outsourcing customer will no longer be guaranteed. For example, granting administrative authorisations to employees of the outsourcing service provider in an uncontrolled manner may result in severe security risks. The employees may exploit the authorisations and copy or manipulate sensitive information.

Non-Existent or Inadequate Testing and Approval Procedures

If an outsourcing customer has not defined any appropriate requirements regarding testing and approval procedures for the outsourcing service provider, existing errors in the hardware and software or vulnerabilities in the configuration might not be detected in time (or at all). This shortcoming may make it impossible to guarantee the necessary protection of the information of the outsourcing customer. Testing may reveal that new components or updates significantly change workflows or require more resources (e.g. main memory, processor capacity) to achieve an acceptable processing speed. If the customer is not informed of this in good time, it can lead to a significant waste of investment or the need to make a significant additional investment.

Unsatisfactory Contractual Arrangements with an Outsourcing Service Provider

Unsatisfactory contractual arrangements with an outsourcing service provider may result in manifold and even severe security issues. If tasks, performance parameters or efforts have been described insufficiently or ambiguously, security safeguards may not be implemented due to ignorance or lack of resources. This may have various negative consequences, such as non-compliance with regulatory requirements and obligations, non-compliance with the duty to provide information and with laws and failures in management commitment due to the loss of control opportunities.

Insufficient Terms for the End of an Outsourcing Project

Without sufficient and appropriate terms regarding the termination of an outsourcing contract by the outsourcing customer, there is the risk that the outsourcing customer will find it

difficult to terminate the business relationship with the outsourcing service provider. This can also happen the other way around, where the outsourcing customer is forced to select an inappropriate outsourcing service provider because the previous outsourcing service provider had the option to terminate the agreement on short notice. In both cases, it may be difficult (if not impossible) to transfer the outsourced area to another service provider or reintegrate it into one's own organisation. This can lead to a wide variety of security problems. During the termination process, for example, data and systems might no longer be protected adequately due to their being considered "legacy systems". Inadequate terms regarding the deletion of data (including backups) might result in confidential data being disclosed to third parties.

Dependency on the Outsourcing Service Provider

The decision to engage in outsourcing always renders the organisation dependent on the outsourcing service provider. This dependency is associated with the risk of losing knowledge and complete control of the outsourced processes and components. Furthermore, it is possible that the protection needs of the outsourced business processes and information are evaluated differently and that the implemented security safeguards are insufficient as a consequence. Since the outsourcing service provider has complete control over business processes, sensitive information, resources and IT systems (while the outsourcing customer's knowledge of these aspects lessens), information security deficits may no longer be noticed in some circumstances.

This situation might be exploited by the outsourcing service provider in the form of significant price increases and a substandard service quality, for example.

Disruption of the Office Climate Due to an Outsourcing Project

Outsourcing projects are often deemed negative changes by the employees of the outsourcing organisation. This frequently results in a poor office climate. The employees of the outsourcing customer often fear changes in tasks that will put them at a disadvantage, or the possibility that outsourcing projects will lead to job cuts. If an outsourcing project comes to be viewed in a negative light, employees might accidentally or wilfully neglect security safeguards, adopt a boycotting attitude or even take revenge in some way. In addition, this could prompt those with specific expertise (such as the Head of IT and the IT Operation Department) to give notice during the introduction phase so that the outsourcing project cannot be implemented as planned.

Poor Information Security in the Initial Outsourcing Phase

The introduction phase of outsourcing projects is frequently characterised by narrow schedule-related and financial specifications. This may result in a lack of security checks and audits, or in reviews and additional quality assurance safeguards not being performed (e.g. when drawing up security concepts). Transitional safeguards with security shortcomings may become routine over the course of time and be maintained for many years due to resource bottlenecks. This results in the specific risk of a "project climate" establishing itself, which causes additional serious security shortcomings.

Failure of an Outsourcing Service Provider's Systems

With an outsourcing service provider, the IT systems and processes operated might fail partially or completely, which also has an impact on the outsourcing customer. If clients are not sufficiently separated, the failure of a system not assigned to the outsourcing customer may, under some circumstances, prevent the outsourcing customer from using the contractually

stipulated service. Similar problems arise when the connection between the outsourcing service provider and customer fails.

Vulnerabilities in the Connection to an Outsourcing Service Provider

If, within the framework of an outsourcing project, the IT connection between the outsourcing service provider and the outsourcing customer is secured insufficiently, the confidentiality and integrity of the data transmitted may be endangered. However, open or poorly secured interfaces might also result in unauthorised access options for third parties regarding the systems of the organisations involved.

Lack of Multi-Client Capability with the Outsourcing Service Provider

Outsourcing service providers normally have numerous different customers that rely on the same resource base (e.g. IT systems, networks, personnel). If the IT systems and data of the different customers are not separated with a sufficient level of security, there is the risk that a customer may access the area of another customer. Furthermore, there might be conflicts of interest on the part of the outsourcing service provider if comparable resource requirements must be met simultaneously. If the respective customers are in a competitive situation, this may be particularly problematic.

Requirements

The specific requirements of module OPS.2.1 *Outsourcing for Customers* are listed below. As a matter of principle, the Head of IT is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of IT
Further Roles	Head of Personnel, IT Operation Department, BCM Officer, Head of Procurement, Change Manager, Head of Organisation, Process Owner

Basic Requirements

For module OPS.2.1 *Outsourcing for Customers*, the following requirements **MUST** be implemented as a matter of priority:

OPS.2.1.A1 Specification of Security Requirements for Outsourcing Projects

All security requirements for an outsourcing project **MUST** be specified on the basis of the outsourcing strategy. Both outsourcing parties **MUST** be contractually obliged to comply with IT-Grundschutz or a comparable level of protection. All interfaces between the outsourcing service provider and the outsourcing customer **MUST** be identified and corresponding security requirements **MUST** be clearly defined in this regard. In the security requirements, it **MUST** be defined which authorisations (site, system, and data access rights) are to be configured in each case.

Standard Requirements

For module OPS.2.1 *Outsourcing for Customers*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

OPS.2.1.A2 Timely Involvement of Employee Representatives [Head of Organisation]

The Employee Representatives SHOULD be informed of an outsourcing project in good time. The Employee Representatives SHOULD already be involved in the tender phase. Depending on the outsourcing project, the statutory rights of co-determination SHOULD be taken into consideration.

OPS.2.1.A3 Selection of a Suitable Outsourcing Service Provider

A requirements profile containing the security requirements for the outsourcing project SHOULD exist for selecting the outsourcing service provider. Evaluation criteria for the outsourcing service provider and its personnel SHOULD exist that are based on this requirements profile.

OPS.2.1.A4 Contractual Arrangements with the Outsourcing Service Provider

All aspects of the outsourcing project SHOULD be agreed in writing with the outsourcing service provider. All roles and cooperation duties (pertaining to persons, for example) for creating, reviewing and changing the security concept SHOULD be agreed with the outsourcing service provider. The rights and obligations of the contractual parties SHOULD be agreed in writing. The outsourcing service provider SHOULD provide the outsourcing customer with the option of performing audits to assess the provider's compliance with the requirements on a regular basis.

OPS.2.1.A5 Determining an Outsourcing Strategy

An outsourcing strategy SHOULD be defined that takes into consideration the relevant aspects of information security in addition to the economic, technical, organisational and legal framework conditions. It SHOULD be clarified which business processes, tasks or applications generally come into question for outsourcing. The outsourcing customer SHOULD retain sufficient capabilities, competencies and resources in order to be able to determine and control the requirements in the field of information security in every outsourcing project. The goals, opportunities and risks of the outsourcing project SHOULD be described in the outsourcing strategy.

OPS.2.1.A6 Drawing up a Security Concept for the Outsourcing Project [Process Owner]

The outsourcing customer SHOULD draw up an information security concept based on the associated security requirements for every outsourcing project. Every outsourcing service provider SHOULD also provide an individual security concept for the respective outsourcing project. The two security concepts SHOULD be coordinated. The security concept of the outsourcing service provider and its implementation SHOULD be consolidated to form an overall security concept and checked for efficiency by the outsourcing customer or independent third parties at regular intervals.

OPS.2.1.A7 Determination of Possible Communication Partners [Head of Organisation]

It SHOULD be defined which internal and external communication partners may transmit and receive which information about the respective outsourcing project. There SHOULD be a process that can be used to check the functionality of the communication partners on both sides.

The admissible communication partners and their respective authorisations **MUST** always be documented and kept up to date.

OPS.2.1.A8 Provisions for Deploying the Personnel of the Outsourcing Service Provider [Head of Personnel]

The employees of the outsourcing service provider **SHOULD** be obliged in writing to comply with the relevant laws and regulations, as well as with the provisions of the outsourcing customer. The employees of the outsourcing service provider **SHOULD** be instructed regarding their tasks and informed of existing information security regulations in a controlled manner. Stand-in arrangements **SHOULD** be in place for the employees of the outsourcing service provider. There **SHOULD** be a controlled process for terminating the contract relationship with the employees of the outsourcing service provider. Third-party personnel deployed by the outsourcing service provider on short notice (or once only) **SHOULD** be treated as visitors.

OPS.2.1.A9 Agreements on Connecting to Outsourcing Partner Networks

Before the network of the outsourcing customer is connected to the network of the outsourcing service provider, all security-relevant aspects **SHOULD** be agreed in writing. The agreement **SHOULD** specifically define the areas and services to which the outsourcing service provider will be granted access in the network of the outsourcing customer. The affected areas **SHOULD** be suitably separated from each other. Compliance with the agreements on the network connection **SHOULD** be checked and documented. Contact partners **SHOULD** be appointed on both sides for organisational and technical questions regarding the network connection. The required security level **SHOULD** be ensured and verified with the outsourcing service provider before the network connection to the outsourcing service provider is activated. In the event of security issues on one or both sides, it **SHOULD** be specified who must be informed and what escalation steps are to be initiated.

OPS.2.1.A10 Agreement on the Exchange of Data Between the Outsourcing Partners

The required security safeguards **SHOULD** be agreed for regular exchanges of data with fixed communication partners. Data formats and approaches for the secure exchange of data **SHOULD** be defined. Contact partners **SHOULD** be appointed for both organisational and technical problems, and especially for security-relevant events when exchanging data with third parties. Availabilities and response times when exchanging data with third parties **SHOULD** be agreed. It **SHOULD** be defined which exchanged data may be used for what purposes.

OPS.2.1.A11 Planning and Continuity of Information Security During Ongoing Outsourcing Operations

An operational concept for the outsourcing project **SHOULD** be drawn up which also takes the security aspects into account. The security concepts of the outsourcing partners **SHOULD** be checked for currency and consistency at regular intervals. The status of the security safeguards agreed **SHOULD** be checked at regular intervals. Regular communications, including coordination regarding changes and improvements, **SHOULD** be performed between the outsourcing partners.

The outsourcing partners **SHOULD** perform regular joint drills and tests to maintain the security level. Information on security risks and how to handle them **SHOULD** be exchanged between the outsourcing partners at regular intervals. There **SHOULD** be a process that secures the flow of information when handling security incidents that affect the respective contractual partners.

OPS.2.1.A12 Change Management [IT Operation Department, Change Manager]

The outsourcing customer SHOULD be given sufficient notice of major changes. The outsourcing customer SHOULD regularly request documentation of all significant changes regarding planning, testing, approval and documentation. Before any changes are made, fallback solutions SHOULD be developed in cooperation with the outsourcing service provider.

OPS.2.1.A13 Secure Migration in Outsourcing Projects

A security management team consisting of qualified employees of the outsourcing customer and the outsourcing service provider SHOULD be established for the migration phase. For the migration phase, a preliminary security concept SHOULD be drawn up that also considers the test and introduction phase. It SHOULD be ensured that production data is not used as test data in an unprotected manner during the migration phase. All changes SHOULD be documented. Upon completion of the migration, the security concept SHOULD be updated. It SHOULD be ensured that all exceptions are reversed at the end of the migration phase. In the event of changes during the migration phase, the extent to which there is a need for an adaptation regarding the contractual bases SHOULD be checked.

OPS.2.1.A14 Contingency Planning for Outsourcing [BCM Officer]

A contingency planning concept for outsourcing SHOULD exist that covers the components of the outsourcing customer and the outsourcing service provider, as well as the associated interfaces and communication channels. The contingency planning concept for outsourcing SHOULD specify the responsibilities, contact persons and processes between the outsourcing customer and the outsourcing service provider. The outsourcing customer SHOULD check the business continuity safeguards implemented by the outsourcing service provider. To this end, joint emergency drills SHOULD be performed by the outsourcing customer and outsourcing service provider.

OPS.2.1.A15 Orderly Termination of an Outsourcing Relationship [Head of Procurement]

The contract with the outsourcing service provider SHOULD specify all aspects regarding the termination of the service relationship, including for both planned and unplanned termination of the contract. It SHOULD be ensured that the termination of the service relationship with the outsourcing service provider will not impair the outsourcing customer's business activities.

All information and data SHOULD be returned to the outsourcing customer upon termination. The outsourcing service provider SHOULD securely delete all related data once this information and data has been returned.

Requirement in Case of Increased Protection Needs

Generic suggestions for module OPS.2.1 *Outsourcing for Customers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.2.1.A16 Security Vetting of Employees (CI)

There SHOULD be contractual agreements with outsourcing service providers that state that the trustworthiness of the personnel deployed will be checked appropriately. To this end, the provider and customer SHOULD work together to define corresponding criteria.

Additional Information

For more information about threats and security safeguards for module OPS.2.1 *Outsourcing for Customers*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[BVIT2005]	Leitfaden Business Process Outsourcing: BPO als Chance für den Standort Deutschland, [Business Process Outsourcing Guide: BPO as an Opportunity for Germany as a Business Location], Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Federal Association for Information Technology, Telecommunications and New Media) (Bitkom), Version 10.1, September 2005, https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Business-Process-Outsourcing.html , last accessed on 26.07.2018
[BVIT2008]	Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis [Guide, Legal Aspects of Outsourcing in Practice]: Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Federal Association for Information Technology, Telecommunications and New Media) (Bitkom), January 2008, https://www.bitkom.org/Bitkom/Publikationen/Rechtliche-Aspekte-von-Outsourcing-in-der-Praxis.html , last accessed on 26.07.2018
[DIN37500]	DIN ISO 37500:2015-08 Guidance on Outsourcing: August 2015
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nist-pubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 15.11.2017

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.2.1 *Outsourcing for Customers*:

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.35 Coercion, Blackmail or Corruption

G 0.42 Social Engineering

Elementary Threats Requirements	G 0.11	G 0.14	G 0.15	G 0.17	G 0.18	G 0.19	G 0.22	G 0.25	G 0.29	G 0.35	G 0.42
OPS.2.1.A1					X				X		
OPS.2.1.A2									X		
OPS.2.1.A3	X										
OPS.2.1.A4									X		
OPS.2.1.A5	X				X				X		
OPS.2.1.A6				X	X	X	X	X	X		
OPS.2.1.A7		X				X					X
OPS.2.1.A8						X			X		
OPS.2.1.A9	X		X		X						
OPS.2.1.A10		X	X	X		X	X				
OPS.2.1.A11						X					
OPS.2.1.A12					X						
OPS.2.1.A13					X	X					
OPS.2.1.A14	X							X			
OPS.2.1.A15	X										
OPS.2.1.A16									X	X	



OPS.2.2: Cloud Usage

Description

Introduction

Cloud computing is understood as offering, using and billing IT services that are dynamically adapted to the customer's requirements via a network. These services are only offered and used by means of defined technical interfaces and protocols. The range of the services offered within the cloud computing framework covers the entire spectrum of information technology, including infrastructure (e.g. computing power, storage space), platforms and software.

Cloud computing offers many advantages: IT services can be used in a need-based, scalable and flexible manner and billed according to the range of functions, service life and number of users in question. In practice, however, the benefits that organisations expect from cloud use often do not fully materialise. This is usually because factors critical to success were not sufficiently considered. Cloud services must therefore be strategically planned and (security) requirements, responsibilities and interfaces carefully defined and agreed. Awareness and understanding of the necessarily changed roles, both on the part of the IT Operation Department and the User, is also an important success factor.

In addition, a number of governance issues are important when introducing cloud services. Examples of this include the implementation of multi-client capability, contractual arrangements, ensuring the portability of different services, billing of the services used, monitoring of the rendering of services, security incident management and numerous aspects of data protection.

Objective

The module describes requirements that allow secure use of cloud services. It is aimed at all organisations that already use such services or want to use them in the future.

Not in Scope

Cloud services represent a special form of outsourcing in almost all delivery models, apart from the use of an on-premise private cloud (see module OPS.2.1 *Outsourcing for Customers*). The threats and requirements described in the module on cloud usage are therefore also often applied within the outsourcing framework. However, cloud services have some special features that are only found in this module. The threats and requirements described here apply regardless of the service and delivery model used.

Security requirements that providers can use to protect their cloud services are not covered by this module, but are covered by the module OPS.3.2 *Cloud Service Providers*. Threats and specific security requirements which must be considered relevant due to the connection of a

cloud service via corresponding application programming interfaces (APIs) are also not covered in the Cloud Usage module. These are covered in the module APP.3.5 *Web Services*.

What distinguishes cloud computing from conventional IT outsourcing?

When the work, production or business processes of an organisation are outsourced, they are dealt with completely or partially by external service providers. This is an established part of organisational strategies today. In most cases, conventional IT outsourcing is designed so that all the infrastructure rented is used exclusively by a single customer (single-tenant architecture) even if outsourcing providers usually have several customers. Moreover, outsourcing contracts are most often concluded over longer periods of time.

Using cloud services is similar to conventional outsourcing in many respects, but there are also several differences which have to be taken into account:

- For economic reasons, several users share a jointly used infrastructure in a cloud.
- Cloud services are dynamic and thus scalable in both directions within much shorter periods. Cloud-based offers can thus be adapted more quickly to the user's actual needs.
- The cloud services used are usually controlled by the cloud user via a web interface. This means that the user can automatically tailor the services used to their individual needs.
- With the technologies used for cloud computing, it is possible to distribute IT performance dynamically over several locations that can be widely distributed geographically (both at home and abroad).
- The customer can easily manage the services used and their resources via web interfaces or other suitable interfaces, which requires little interaction with the provider.

Threat Landscape

For module OPS.2.2 *Cloud Usage*, the following specific threats and vulnerabilities are of particular importance:

Non-existent or Insufficient Strategy for Cloud Use

Using cloud services in an organisation is a strategic decision. A non-existent or insufficient strategy for cloud use makes it possible for an organisation to choose an inappropriate cloud service or provider. The selected cloud service may not be compatible with the organisation's own IT, internal business processes or protection needs. This can have a negative impact on business processes in organisational, technical, or financial terms. In general, a non-existent or inadequate strategy for cloud use can result in the associated objectives not being achieved or the security level falling significantly.

Dependence on a Cloud Service Provider (Loss of Control)

If an organisation uses external cloud services, it is more or less dependent on the respective cloud service provider. As a result, the organisation may no longer be able to fully control the outsourced business processes or the associated information – or, in particular, their security. Despite possible controls, the organisation is also dependent at a certain point on the cloud

service provider's correct implementation of security measures. Failure in this regard results in inadequate protection of business processes and business-critical information.

In addition, the use of external cloud services can lead to the loss of knowledge about information security and technology within the organisation. As a result, the organisation may no longer be able to assess whether the protective measures taken by the provider are sufficient. Even a change of provider is very difficult to achieve. The cloud service provider could also use this leverage to push through price increases or reduce the quality of its service, for example.

Poor Compliance Management When Using the Cloud

When an organisation decides to use a cloud service, the decision usually carries lots of expectations. For example, employees are hoping for higher performance or greater functionality from outsourced services, while management is betting on lower costs. However, a lack of compliance management prior to cloud use can lead to expectations not being met and the service not delivering the desired added value (e.g. in terms of availability).

Violations of Legal Provisions

Many cloud service providers offer their services in an international environment. They are thus often subject to other national legislation. Cloud customers often only see the advantages associated with cloud computing (e.g. cost advantages) and misjudge the legal framework conditions to be observed with regard to aspects such as data protection, information obligations, insolvency law, liability or information access for third parties. This could result in violations of applicable policies and regulations and compromise the security of outsourced information.

Cloud Service Providers Offering Inadequate Multi-Client Capability

In cloud computing, different customers usually share a common infrastructure, such as IT systems, networks and applications. If the resources of the different customers are not separated securely enough, a customer may be able to access the areas of another customer and manipulate or delete information there.

Unsatisfactory Contractual Arrangements with a Cloud Service Provider

Unsatisfactory contractual arrangements with a cloud service provider may result in manifold and even severe security issues. If areas of responsibility, tasks, performance parameters or efforts are described insufficiently or ambiguously, it is possible that the cloud service provider will not implement security measures at all or only insufficiently due to a lack of resources.

The customer may also be put at a disadvantage by situations which are not clearly regulated by contract. For example, cloud service providers often use third-party services in rendering their own services. If there are insufficient contractual agreements or if the dependencies between the service provider and third party have not been disclosed, this can also have a negative effect on information security and the service provided to the organisation.

Lack of Planning of Migrations to Cloud Services

Migrating to a cloud service is almost always a trying phase. Poor planning can lead to errors that affect information security within the organisation. If, for example, an organisation recklessly dispenses with a gradual migration due to an insufficient planning phase, this can lead to considerable problems in practice. Without test phases, pilot users or temporary parallel opera-

tion of the existing infrastructure and cloud services, data can be lost or services can fail completely.

Inadequate Integration of Cloud Services into the Organisation's Own IT

Cloud services must be adequately integrated into the organisation's IT infrastructure. If the persons in charge do not implement this sufficiently, users may not be able to fully access the cloud services that have been commissioned. The cloud services may thus not deliver the required and agreed performance, or they may not be accessible (or only to a limited extent). This can slow down business processes or cause them to fail altogether. If cloud services are improperly integrated into an organisation's in-house IT, serious vulnerabilities can also arise.

Insufficient Provisions for Termination of the Cloud Project

Inadequate provisions for potential termination of a contract can have serious consequences for the organisation. Experience has shown that this is always particularly problematic if a case that is critical from the organisation's point of view occurs unexpectedly, such as the bankruptcy or sale of the cloud service provider or serious security concerns. Without adequate internal precautions and detailed contract provisions, the organisation will have difficulty terminating the contract concluded with the cloud service provider. In this case, it may be difficult (if not impossible) to transfer the outsourced cloud service promptly to another service provider, for example, or to reintegrate it back into the organisation.

Moreover, insufficiently regulated data deletion at the end of the contract may lead to unauthorised access to an organisation's information.

Inadequate Administration Model for Cloud Use

Cloud services often change the understanding of roles within an organisation's IT Operation Department. The role of administrator often evolves from a conventional system administrator into a service administrator. If this process is not sufficiently supported, it can have a negative effect. For example, the administrators may not have the necessary understanding of the conversions required, or they may not have been adequately trained for their new roles. As a result, the cloud services may not be properly administered and thus only be available to a limited extent, or they may fail altogether.

Insufficient Contingency Planning Concept

An insufficient contingency planning concept can quickly lead to serious consequences when using the cloud. If the cloud service or parts of it fail, then failings in the contingency planning concepts of the cloud service provider and the interfaces always lead to unnecessarily long downtimes, with corresponding consequences for the customer's productivity or services. In addition, poor coordination of emergency scenarios between the customer and the service provider may cause gaps in contingency planning.

Failure in the IT Systems of a Cloud Service Provider

With a cloud service provider, the IT systems, applications and processes operated might fail partially or completely, which also has an impact on the cloud customer. If the clients are insufficiently separated, even a failed IT system that is not assigned to the cloud customer can result in the cloud customer no longer being able to access the contractually guaranteed service. Similar problems arise when the connection between the cloud service provider and the customer fails, or when the cloud computing platform in use is successfully attacked.

Requirements

The specific requirements of module OPS.2.2 *Cloud Usage* are listed below. As a matter of principle, the Head of IT is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of IT
Further Roles	Head of Personnel, Data Protection Officer, IT Operation Department, Top Management, Process Owner

Basic Requirements

For module OPS.2.2 *Cloud Usage*, the following requirements **MUST** be implemented as a matter of priority:

OPS.2.2.A1 Drawing up a strategy for cloud usage [Process Owner, Top Management, Data Protection Officer]

A strategy for cloud use **MUST** be drawn up. It **MUST** define the objectives, opportunities and risks that the organisation associates with cloud use. In addition, the legal and organisational framework conditions and the technical requirements arising from the use of cloud services **MUST** be examined. The results of this investigation **MUST** be documented in a feasibility study.

The services to be purchased from a cloud service provider in the future **MUST** be documented along with the chosen delivery model. In addition, it **MUST** be ensured that all fundamental technical and organisational security aspects are sufficiently considered in the planning phase for cloud use.

A rough individual security analysis **SHOULD** be carried out for the planned cloud service. This **SHOULD** be repeated if technical and organisational framework conditions change significantly. For larger cloud projects, a roadmap **SHOULD** also be developed to determine when and how a cloud service will be deployed.

OPS.2.2.A2 Drawing up a security policy for cloud usage [Process Owner]

Based on the cloud use strategy (see OPS.2.2.A1 *Drawing up a strategy for cloud usage*), a security policy for cloud usage **MUST** be created. It **MUST** include specific security requirements for implementing cloud services within the organisation. It **MUST** also document specific security requirements for the cloud service provider and the defined level of protection for cloud services in terms of confidentiality, integrity and availability. If cloud services from international providers are used, the special country-specific requirements and legal regulations **MUST** be taken into account.

OPS.2.2.A3 Service definition for cloud services by the user [Process Owner]

A service definition **MUST** be developed for each cloud service. All planned and used cloud services **SHOULD** also be documented.

OPS.2.2.A4 Definition of areas of responsibility and interfaces [Process Owner]

Based on the service definition for cloud services (see OPS.2.2.A3 *Service definition for cloud services by the user*), the organisation **MUST** identify and document all relevant interfaces and responsibilities for cloud use. It **MUST** clearly show how the responsibilities of cloud service providers and customers are separated from each other.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module OPS.2.2 *Cloud Usage*: They **SHOULD** be implemented as a matter of principle.

OPS.2.2.A5 Planning a secure migration to a cloud service [Process Owner]

Before migrating to a cloud service, a migration concept **SHOULD** be drawn up. To enable this, organisational regulations and the distribution of tasks **SHOULD** first be defined. In addition, existing business processes with respect to cloud use **SHOULD** be identified and adjusted. It **SHOULD** be ensured that the organisation's own IT is sufficiently considered in the migration process. Those in charge **SHOULD** also determine whether the organisation's employees should receive additional training.

OPS.2.2.A6 Planning the secure integration of cloud services [IT Operation Department]

Before using a cloud service, careful planning **SHOULD** be undertaken regarding how it is to be integrated into the organisation's IT. For this purpose, the following areas at minimum **SHOULD** be examined as to whether adjustments are necessary: interfaces, network connection, administration model, data management model. The results **SHOULD** be documented and updated at regular intervals.

OPS.2.2.A7 Drawing up a security concept for cloud usage [IT Operation Department]

A security concept for the use of cloud services **SHOULD** be developed based on the security requirements identified (see OPS.2.2.A2 *Drawing up a security policy for cloud usage*).

OPS.2.2.A8 Careful selection of a cloud service provider [Top Management]

A detailed requirements profile for a cloud service provider **SHOULD** be created based on the service definition for the cloud service (see OPS.2.2.A3 *Service definition for cloud services by the user*). A service specification and a requirements specification **SHOULD** be drawn up. Supplementary sources of information **SHOULD** also be used to evaluate a cloud service provider. The available service descriptions of the cloud service provider **SHOULD** also be carefully examined and reviewed.

OPS.2.2.A9 Contractual arrangements with the cloud service provider [Top Management]

The contractual provisions between the organisation and the cloud service provider **SHOULD** be adapted in type, scope and level of detail to the protection needs of the information to be used in the cloud. The location in which the cloud service provider renders its services **SHOULD** be specified. In addition, escalation levels and communication channels **SHOULD** be defined between the organisation and the cloud service provider. The manner in which the organisation's data should be securely deleted **SHOULD** also be agreed. Likewise, termination

provisions SHOULD be established in writing. The cloud service provider SHOULD disclose all the subcontractors it requires for the cloud service.

OPS.2.2.A10 Secure migration to a cloud service [Process Owner, IT Operation Department]

The migration to a cloud service SHOULD be based on the migration concept drawn up (see OPS.2.2.A5 *Planning the secure migration to a cloud service*). During the migration, the security concept for cloud usage SHOULD be checked in case it needs to be adapted to any new requirements (see OPS.2.2.A7 *Drawing up a security concept for cloud usage*). All preventive safeguards for contingency SHOULD also be complete and up-to-date.

The migration to a cloud service SHOULD first be verified by a test. Once the cloud service has gone live, whether the cloud service provider meets the organisation's defined requirements SHOULD be checked.

OPS.2.2.A11 Drawing up a contingency concept for a cloud service [IT Operation Department]

A contingency concept SHOULD be created for the cloud services used. It SHOULD contain all necessary information about responsibilities and contact persons. In addition, detailed rules SHOULD be drawn up for backups. The specifications for redundant management tools and interface systems SHOULD also be recorded.

OPS.2.2.A12 Information security continuity during live cloud operations [IT Operation Department]

All documentation and policies created for the cloud services in use SHOULD be updated regularly. The organisation SHOULD also periodically check whether the cloud service provider is rendering the contractually guaranteed services. If possible, the cloud service provider and the user organisation SHOULD also coordinate on a regular basis. Plans SHOULD be made and drills carried out on how to respond to system failures.

OPS.2.2.A13 Evidence of sufficient information security for cloud usage

The organisation SHOULD have the cloud service provider regularly prove that the agreed security requirements are being met. The evidence SHOULD be based on an internationally recognised set of rules (e.g. ISO/IEC 27001, IT-Grundschutz, Compliance Control Catalogue (C5), Cloud Controls Matrix of the Cloud Security Alliance). The organisation SHOULD check whether the scope and protection needs cover the cloud services used.

If a cloud service provider uses subcontractors to provide the cloud services, it SHOULD regularly demonstrate to the organisation that these subcontractors are performing the necessary audits.

OPS.2.2.A14 Orderly termination of a cloud service relationship [Process Owner, Top Management]

If a service relationship with a cloud service provider is terminated, it SHOULD be ensured that this will not interfere with the business operations of the organisation. The contract with the cloud service provider SHOULD regulate how the service relationship can be terminated in an orderly manner.

Requirement in Case of Increased Protection Needs

Generic suggestions for module OPS.2.2 *Cloud Usage* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.2.2.A15 Portability of cloud services [Process Owner, IT Operation Department] (A)

All the requirements necessary to change cloud service providers or bring the cloud service or data back into the organisation's own IT infrastructure SHOULD be defined. Portability tests SHOULD also be performed regularly. The contract with the cloud service provider SHOULD include specifications to ensure the necessary portability.

OPS.2.2.A16 Implementing in-house backups [Process Owner, IT Operation Department] (IA)

The organisation SHOULD check whether it should create its own backups in addition to those the cloud service provider is contractually obligated to create. In addition, detailed requirements SHOULD be created for a backup service.

OPS.2.2.A17 Use of encryption when using the cloud [IT Operation Department] (IA)

If data is encrypted by a cloud service provider, the encryption mechanisms and key lengths that may be used SHOULD be contractually agreed. If the organisation's own encryption mechanisms are used, suitable key management SHOULD be ensured. The encryption SHOULD take into account any special features of the selected cloud service model.

OPS.2.2.A18 Use of federation services [Process Owner, IT Operation Department] (CIA)

The organisation SHOULD check whether Federation Services are being used in a cloud computing project.

It SHOULD be ensured that a Security Assertion Markup Language (SAML) ticket only transmits the necessary information to the cloud service provider. The authorisations SHOULD be checked regularly so that only authorised users are issued an SAML ticket.

OPS.2.2.A19 Security vetting of employees [Head of Personnel] (CIA)

There SHOULD be contractual agreements with cloud service providers stating that the qualifications and trustworthiness of the personnel deployed will be suitably checked. To this end, an organisation SHOULD work with its cloud service provider to define corresponding criteria.

Additional Information

For more information about threats and security safeguards for module OPS.2.2 *Cloud Usage*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[BSIC5]	Cloud Computing Requirements Catalogue (C5): (BSI), Kriterien zur Beurteilung der

	Informationssicherheit von Cloud-Diensten, Federal Office for Information Security (BSI), September 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Anforderungskatalog-Cloud_Computing-C5.pdf , last accessed on 30.08.2018
[CSA]	Security Guidance for Critical Areas of Focus in Cloud Computing: Cloud Security Alliance (CSA), Version 4.0, 2017, https://cloudsecurityalliance.org/download/security-guidance-v4/ , last accessed on 30.08.2018
[ENISA]	Cloud Computing: Benefits, Risks and Recommendations for Information Security: European Union Agency for Network and Information Security (ENISA), November 2009, https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport , last accessed on 30.08.2018
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NIST800144]	Guidelines on Security and Privacy in Public Cloud Computing: NIST Special Publication 800-144, December 2011, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf , last accessed on 30.08.2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 15.11.2017

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.2.2 *Cloud Usage*:

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices Or Systems

G 0.26 Malfunction of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.35 Coercion, Blackmail or Corruption

G 0.40 Denial of Service

G 0.45 Data Loss

Elementary Threats Requirements	G 0.9	G 0.11	G 0.14	G 0.15	G 0.18	G 0.19	G 0.22	G 0.25	G 0.26	G 0.29	G 0.30	G 0.32	G 0.35	G 0.40	G 0.45
OPS.2.2.A1		X			X					X					
OPS.2.2.A2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
OPS.2.2.A3					X					X					
OPS.2.2.A4					X			X	X						
OPS.2.2.A5					X	X		X	X						
OPS.2.2.A6					X	X		X	X						
OPS.2.2.A7	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
OPS.2.2.A8		X													
OPS.2.2.A9		X			X					X					
OPS.2.2.A10					X	X		X	X						
OPS.2.2.A11	X	X						X	X						
OPS.2.2.A12					X			X	X	X	X	X			
OPS.2.2.A13					X			X	X	X	X	X			
OPS.2.2.A14		X													
OPS.2.2.A15		X						X	X						
OPS.2.2.A16		X													X
OPS.2.2.A17			X	X											
OPS.2.2.A18											X	X			
OPS.2.2.A19			X			X				X	X	X	X		



OPS.2.4: Remote Maintenance

Description

Introduction

The term "remote maintenance" refers to physically separate access to IT systems and the applications running on them for configuration, maintenance, repair or control purposes. Remote maintenance can be performed passively by solely observing access to the IT system or the applications, or actively through direct administrative intervention in the operating system or running applications. In the case of passive remote maintenance, a user must perform the actual actions on site under the guidance of an administrator. Active remote maintenance, on the other hand, involves direct intervention in an operating system by an administrator. Among other things, mouse input, keyboard commands, display contents and console output are transmitted. Even if effective mechanisms to protect the remote maintenance access are implemented, there are ways to directly access the internal network and the data processed there from the outside. These interfaces may be used by third parties in order to endanger the organisation and thus cause economic and operational damage.

Objective

The objective of this module is to protect the information stored, processed and transmitted on the basis of remote maintenance. For this purpose, requirements are imposed that relate to functions of active and passive remote maintenance.

Not in Scope

This module covers remote maintenance from the point of view of the IT Operation Department and provides advice for users as to how remote maintenance may be used. It is important to holistically guarantee information security in all lifecycle phases. The security aspects of the communication links used, the authentication mechanisms and protection of remote maintenance access are important components of the module. Module OPS.2.4 *Remote Maintenance* does not cover all the relevant aspects of the related business processes. In particular, aspects of the modules OPS.1.1.3 *Patch and Change Management*, ORP.3 *Awareness and Training*, CON.1 *Crypto Concept* and CON.3 *Backup Concept* must thus be ensured separately. The specifications of the module layers NET (*Networks and Communication*) and DER (*Detection and Reaction*), the modules of the layer OPS.2 *Operation Through Third Parties* and the modules of the layer OPS.3 *Outsourcing for Third Parties* that are directly related to remote administration must be implemented, as well. In the case of cloud-based products, module OPS.2.2 *Cloud Usage* must be considered. The remote procedure calls of Windows 2010 are not covered in this module either.

Threat Landscape

For module OPS.2.4 *Remote Maintenance*, the following specific threats and vulnerabilities are of particular importance:

Inadequate Knowledge of Remote Maintenance Regulations

If the persons involved have inadequate knowledge of important regulations and do not follow them as a consequence, the protection of information within the framework of remote maintenance will be endangered. Therefore, IT operations will be at risk if applicable regulations are not made generally known. In particular, administrators who set up and use remote maintenance are dependent on regulations (e.g. regarding configurations); otherwise, remote maintenance will create additional operational risks and security vulnerabilities in the internal network and it will not be possible to detect or fend off attacks via remote maintenance.

Non-Existent or Inadequate Planning and Rules for Remote Maintenance

If remote maintenance is not planned, set up and controlled carefully, the security of not just one IT system, but all IT systems of an organisation may be impaired if vulnerabilities are exploited. Vulnerabilities may occur in many areas and may affect communication protocols, patch processes, encryption algorithms and authentication mechanisms. As a consequence of inadequately secured remote maintenance interfaces, an adjacent third-party network may also be compromised.

Unauthorised Use of Rights During Remote Maintenance

Site, system and data access authorisations tailored to the respective tasks are used to protect information, business processes and IT systems against unauthorised access. If these authorisations are granted to unauthorised persons in the case of remote maintenance or rights are remotely exercised in an unauthorised manner, this may result in a large number of threats to the confidentiality and integrity of data and the availability of computing power (for example). Possible damage scenarios include injections of malware, the manipulation of data and information, and the unauthorised gathering of information. The impacts may include financial losses and losses of knowledge, physical destruction of material assets, and compromised IT systems and networks.

Inappropriate Use of Authentication During Remote Maintenance

During remote maintenance, authentication mechanisms which are based on the authentication data stored in the user administration are used. If unauthorised third parties obtain administrative authorisations on remote maintenance computers or for remote maintenance tools, this may cause extensive damage to the organisation. This includes unauthorised configurations of IT systems and applications, compromised systems, and losses of information and data.

Insecure and Uncontrolled Establishment of Communication Links

For remote maintenance, access to communication interfaces of the administered computer is necessary as a matter of principle. This always poses a potential threat.

In the communication interfaces of IT systems, what is being transmitted besides user and log information is not always obvious to the user. Under certain circumstances, a manipulated (or simply activated) communication interface can establish a connection to a remote terminal

without the user's input, or it can be addressed by third parties via a function unknown to the user.

Improper Remote Maintenance

To ensure the security and proper functioning of IT systems and applications which may only be accessed remotely, professional and continuous remote maintenance is required. If IT systems and applications are not properly configured, maintained, repaired and controlled via remote maintenance, they will (in the worst case) no longer be usable. If errors occur within the remote maintenance processes, this may directly result in malfunctions of individual operating system functions. Moreover, vulnerabilities may occur because of IT system maintenance work that was carried out too late or improperly.

Use of Insecure Protocols in Remote Maintenance

Communication via public and internal networks by means of insecure protocols constitutes a potential threat. If, for example, outdated versions of IPSec, SSH or SSL/TLS are used to establish a tunnel between two end points or networks, the security of these tunnels cannot be adequately guaranteed. Attackers may exploit vulnerabilities of these protocols in order to inject their own contents into protected connections. Protocols in which information is transmitted in plain text are generally considered insecure.

Inappropriate Handling of Authentication Methods During Remote Maintenance

The security of an authentication method directly depends on careful handling. The disclosure of user-bound authentication data and the insecure storage of this information constitute a potential threat. Vulnerabilities may arise that allow unauthorised access to the rights and role profiles of the administrators, as well as to IT systems and applications.

Insecure Cryptographic Algorithms for Remote Maintenance

If insecure cryptographic procedures are used or secret keys are not adequately protected, this will result in a loss of security within the framework of remote maintenance. Negligence in the field of cryptographic algorithms may lead to cryptographic keys being compromised. In addition to this, it is easier for attackers to penetrate the system if they can analyse or break the cryptographic procedure used with an acceptable amount of time and technical resources and gain access to communications as a result.

Insecure and Uncontrolled Use of Remote Maintenance Access by Third Parties

If unauthorised or third parties are enabled to use the remote maintenance components without a contractual basis (for example, if access control policies of the organisation are bypassed or not implemented carefully), the security of remote maintenance, IT systems and applications will no longer be guaranteed.

Use of Online Services for Remote Maintenance

In addition to remote maintenance in which an administrator establishes a direct data connection to the organisation to be administered, online services may also be used. In so doing, the IT systems to be administered establish a connection to the servers of a third-party provider and the administrators may use a web browser or similar means to access the IT systems to be administered.

Since the communications are not subject to end-to-end encryption and access is obtained by a third party, the data exchange may be directly intercepted. In addition, the IT systems may also be administered by unauthorised persons if the data connection is manipulated. If the systems automatically establish a data connection to the online service when booting the system and the access credentials are known, direct access to the IT system may be possible.

Establishing a connection to the online service often requires no administrative rights on the IT systems to be administered, which means the administrator only needs a browser. This way, users without administrative rights may gain remote access without being authorised to do so.

Requirements

The specific requirements of module OPS.2.4 *Remote Maintenance* are listed below. As a matter of principle, the Head of IT is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of IT
Further Roles	IT Operation Department, User

Basic Requirements

For module OPS.2.4 *Remote Maintenance*, the following requirements **MUST** be implemented as a matter of priority:

OPS.2.4.A1 Planning the Use of Remote Maintenance [IT Operation Department]

The use of remote maintenance **MUST** be adapted to the organisation and planned adequately with regard to technical and organisational aspects. It **MUST** be clarified whether in-band or out-band administration is to be used and which IT system interfaces and protocols are to be involved. It **MUST** be clarified how the remote maintenance is to be secured and audited.

OPS.2.4.A2 Establishing a Secure Connection for Remote Maintenance [User]

The remote maintenance access **MUST** be initiated from within the organisation. The user of the remotely administered IT system **MUST** explicitly consent to the remote access.

OPS.2.4.A3 Securing Communication Links for Remote Maintenance [IT Operation Department]

The possible access and communication interfaces for establishing a connection from the outside **MUST** be restricted to those required. All communication links **MUST** also be disconnected after the remote access has been performed (deactivation). The ports necessary for remote maintenance **MUST** be made constantly available. Taking into consideration the required protection needs of the IT system or application, secure authentication mechanisms **MUST** be used for the administrators.

OPS.2.4.A4 Regulations for Communication Links [IT Operation Department]

Taking the firewall requirements of the organisation into account, remote maintenance **MUST** be integrated into the firewall rules. In this respect, it **MUST** be ensured that existing firewall infrastructures and their regulations are not bypassed.

When checking the network connectivity by means of ICMP, the regulations for local and remote tests **MUST** be taken into account.

OPS.2.4.A5 Use of Online Services [IT Operation Department, User]

It **MUST** be decided whether remote maintenance using online services is allowed. The use of online services for remote maintenance **SHOULD** be prohibited. Technical and organisational safeguards **SHOULD** be implemented in order to enforce the ban.

If this use cannot be avoided, it **SHOULD** be restricted to as few cases as possible. The conditions applicable to the use of remote maintenance through online services **SHOULD** be defined. The clients **SHOULD** not be allowed to automatically establish any connections to the online service.

Standard Requirements

For module OPS.2.4 *Remote Maintenance*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

OPS.2.4.A6 Drawing Up a Policy for Remote Maintenance [IT Operation Department]

The regulations for remote maintenance **SHOULD** be documented in a policy. If a separate policy is drawn up, the policy for remote maintenance **SHOULD** be referenced in the existing policies of the organisation. The policy **SHOULD** be known to all persons in charge who are involved in the design, implementation, operation and disposal and provide the basis for their work.

OPS.2.4.A7 Documentation During Remote Maintenance [IT Operation Department]

Up-to-date documentation of remote maintenance **MUST** be available. Existing deputies **SHOULD** be able to take over the relevant tasks and processes at any given point in time. Since the documents contain confidential information and data in most cases, they **SHOULD** be stored in a secure manner in suitable places and also be available within the framework of business continuity management. Protection against unauthorised access to the documentation **SHOULD** also be ensured. All remote access options **SHOULD** be recorded and documented.

OPS.2.4.A8 Secure Protocols for Remote Maintenance [IT Operation Department]

Communication protocols that are up to date and classified as secure **SHOULD** be used. Communications **SHOULD** be encrypted. Based on the protection needs of the organisation, suitable cryptographic procedures **SHOULD** be used to realise a tunnel for this purpose. To ensure that the protocols used can be managed adequately and the security requirements are taken into account, information about vulnerabilities from the specialised press or other relevant sources **SHOULD** be taken into account and continuously updated.

OPS.2.4.A9 Selection of Appropriate Remote Maintenance Tools [IT Operation Department]

Suitable remote maintenance tools SHOULD be selected based on the operational, security-related and data protection requirements of the organisation. All procurement decisions SHOULD be coordinated with the persons in charge of the Procurement Department, the persons in charge of the systems and applications, and security management.

OPS.2.4.A10 Management of Remote Maintenance Tools [IT Operation Department, User]

Organisational management processes describing how to handle the tools selected SHOULD be established. Operating instructions describing how to handle the remote maintenance tools SHOULD be available. Sample procedures for passive and active remote maintenance SHOULD be drawn up and communicated. An effort SHOULD be made to raise the IT Operation Department's awareness of remote maintenance tools and train its members on how to use them. A contact person for all technical issues regarding the remote maintenance tools SHOULD be appointed.

OPS.2.4.A11 Use of Cryptographic Procedures in Remote Maintenance [IT Operation Department]

For remote maintenance, sufficiently strong cryptographic procedures SHOULD be used to secure communications and authenticate the administrators. The strength of the cryptographic procedures and keys used SHOULD be checked at regular intervals within the framework of remote maintenance and adjusted as necessary.

OPS.2.4.A12 Patch and Change Management in Remote Maintenance [IT Operation Department]

The general specifications regarding the patch and change management of the organisation SHOULD be implemented for remote maintenance. The IT systems and administration tools SHOULD be taken into consideration in patch and change management.

The remote maintenance access SHOULD be enabled and disabled in a suitable manner. All activations and deactivations of remote maintenance access SHOULD also be documented. For security reasons, all IT systems and applications maintained by means of remote maintenance SHOULD be patched in a timely manner. Before patches and changes are installed in a production system by means of remote maintenance, they SHOULD be tested in advance in a suitably configured test environment.

OPS.2.4.A13 Backups During Remote Maintenance [IT Operation Department]

In order to avoid data losses within the infrastructure for remote maintenance, backups SHOULD be performed at regular intervals. Backup specifications in the case of remote maintenance SHOULD be made based on the amount and importance of new data that is continuously stored and the possible damage to the organisation should this data be lost.

All backup requirements for remote maintenance SHOULD correspond to the organisation's general specifications regarding backups.

OPS.2.4.A14 Dedicated Systems for Remote Maintenance [IT Operation Department]

Within the framework of remote maintenance, components which only service this application purpose SHOULD be used. All other functions/services SHOULD be deactivated. The remote maintenance components SHOULD be configured securely.

OPS.2.4.A15 Securing Remote Maintenance [IT Operation Department]

Remote maintenance SHOULD only be performed from the internal network.

If it is nevertheless necessary to access internal IT systems from a public data network, a secured virtual private network (VPN) SHOULD be used. For remote maintenance via VPN, a protected data connection to the VPN end point SHOULD be generated. In addition to this external remote maintenance access, the internal remote maintenance access SHOULD be secured. The use of internal remote maintenance access SHOULD be restricted whenever possible. Moreover, all activities during an administration session SHOULD be logged.

OPS.2.4.A16 Training Measures on Remote Maintenance [IT Operation Department]

Adequate knowledge of how to handle the remote maintenance components SHOULD be conveyed to the administrators. These training measures SHOULD be integrated into established procedures of the organisation.

It SHOULD also be pointed out to the employees what they have to observe in the case of remote maintenance.

OPS.2.4.A17 Authentication Mechanisms for Remote Maintenance [IT Operation Department]

For remote maintenance, two-factor methods SHOULD be used for authentication.

The selection of the authentication method and the reasons on which this selection was based SHOULD be documented. In order to make it easier to log in during remote maintenance, this area SHOULD be integrated into identity and access management and its infrastructures.

OPS.2.4.A18 Password Security for Remote Maintenance [IT Operation Department]

If password-based authentication is used for remote maintenance, password rules SHOULD be defined, documented and made known to the administrators. For remote maintenance, these password rules SHOULD be technically enforced.

OPS.2.4.A19 Remote Maintenance by Third Parties [IT Operation Department]

If it is not possible to do without external remote maintenance, all activities within this framework SHOULD be monitored by internal parties. All remote maintenance processes performed by third parties SHOULD be recorded. Contractual arrangements MUST be made with external maintenance personnel, especially regarding the security of the affected IT systems and information. The duties and qualifications of the external maintenance personnel SHOULD be specified in the contract.

OPS.2.4.A20 Remote Maintenance Operations [IT Operation Department]

A reporting process for support and remote maintenance matters SHOULD be established (e.g. a ticket system). All remote maintenance access SHOULD only be permitted after successful authentication.

The security infrastructure activations required to establish remote maintenance access SHOULD be integrated into the established processes for firewall rules. Mechanisms for detecting and thwarting high-volume attacks, TCP state exhaustion attacks and attacks at the application level SHOULD be implemented.

All remote maintenance processes SHOULD be recorded. The resulting log data SHOULD be evaluated regularly.

Requirements in Case of Increased Protection Needs

Generic suggestions for module OPS.2.4 *Remote Maintenance* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.2.4.A21 Creation of a Business Continuity Plan in Case Remote Maintenance Fails (A)

As part of contingency planning, a concept describing how the consequences of a failure of remote maintenance components can be minimised and which activities have to be performed in the event of a failure SHOULD be developed. The business continuity plan SHOULD ensure that disruptions and damage (including damage sustained later on) are minimised and normal operation is restored in a timely manner.

OPS.2.4.A22 Redundant Use of Mobile Communication Networks (A)

For the protection of remote maintenance communication networks in case of high-availability requirements, redundant connection and communication networks SHOULD be configured.

OPS.2.4.A23 Planning Secure Use in a Secured Network Segment [IT Operation Department] (C)

For remote maintenance, a secured network segment SHOULD be used. This SHOULD be realised and operated in the same way as a demilitarised zone (DMZ). Remote maintenance access SHOULD NOT cause existing security infrastructures to be bypassed and trustworthy and non-trustworthy networks to be merged as a consequence.

Additional Information

For more information about threats and security safeguards for module OPS.2.4 *Remote Maintenance*, see the following publications, among others:

[CSE108]	Remote Maintenance in Industrial Environments: BSI Publications on Cyber Security (CSE 108), Version 1.0, January 2015, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_108.pdf , last accessed on 05.10.2018
[CSE54]	Basic Rules for Protecting Remote Maintenance Accesses: BSI Publications on Cyber Security (BSI-CS 054), Version 1.0, June 2013, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_054.pdf , last accessed on 05.10.2018
[TR02102]	Cryptographic Mechanisms: Recommendations and Key Lengths: BSI TR-02102, Federal Office for Information Security (BSI), January 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , last accessed on 13.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.2.4 *Remote Maintenance*:

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.9	G 0.14	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.30	G 0.31	G 0.32	G 0.39	G 0.40	G 0.43	G 0.46
OPS.2.4.A1		X	X	X	X							X	X			X
OPS.2.4.A2		X		X			X	X		X					X	X
OPS.2.4.A3			X				X				X		X			X
OPS.2.4.A4			X			X							X			X
OPS.2.4.A5				X		X		X						X	X	
OPS.2.4.A6			X													
OPS.2.4.A7		X	X	X												
OPS.2.4.A8		X	X	X			X	X					X			X
OPS.2.4.A9			X		X											
OPS.2.4.A10			X		X	X										
OPS.2.4.A11				X	X	X	X	X		X		X				X
OPS.2.4.A12			X		X				X				X	X	X	
OPS.2.4.A13		X							X							X
OPS.2.4.A14			X			X	X	X		X						
OPS.2.4.A15			X	X			X						X			X
OPS.2.4.A16			X		X							X				
OPS.2.4.A17		X		X		X	X	X								
OPS.2.4.A18		X		X		X	X	X		X		X			X	
OPS.2.4.A19				X		X	X			X	X	X				
OPS.2.4.A20			X			X	X	X		X	X	X	X			
OPS.2.4.A21	X		X				X		X				X	X		

OPS.2.4.A22			X	X			X				X					
OPS.2.4.A23		X	X			X				X						



OPS.3.1: Outsourcing for Service Providers

Description

Introduction

Within the framework of outsourcing, outsourcing service providers take over business processes and services (e.g. security or cleaning personnel) entirely or partially from outsourcing customers. The operation of hardware and software may also be taken over as a service. Regardless of the services actually taken over, this requires a close relationship between the outsourcing service provider and the outsourcing customer. The outsourcing service provider is not spared from the risks within the framework of the outsourcing relationship. Normally, the outsourcing service provider must implement the risk-reducing security requirements defined by the outsourcing customer (see module OPS.2.1 *Outsourcing for Customers*). It is in the interest of both the outsourcing customer and the outsourcing service provider to provide the agreed service and meet the level of security stipulated. If the outsourcing service provider fails to meet the requirements imposed on it, it may face high contractual penalties and additional legal consequences that involve not only financial consequences, but reputational damage, as well. This module thus concentrates on requirements that address the processes of planning, implementing and controlling information security aspects within the framework of outsourcing from the service provider's point of view.

Objective

This module describes the requirements an outsourcing service provider needs to fulfil to be able to meet the level of security of the outsourcing organisation and avoid risks resulting from the business relationship that cannot be controlled by the outsourcing service provider.

Not in Scope

The module includes security requirements for outsourcing that must be met by service providers. It complements the requirements regarding the protection of information of the outsourcing organisation from the outsourcing service provider's point of view.

The protection of the transmission channels between the service provider and the outsourcing customer is not addressed within the framework of this module.

The terms "outsourcing" and "cloud" have many parallels. For outsourcing service providers, requirements regarding the use of cloud services must normally be taken into consideration as well.

Threat Landscape

For module OPS.3.1 *Outsourcing for Service Providers*, the following specific threats and vulnerabilities are of particular importance:

Failure of a Wide Area Network (WAN)

Outsourcing service providers that do not operate on site with the customer depend significantly on the availability of wide area networks (WAN). For economic reasons, the services are mostly provided from a few centralised locations. The service provider connects to the outsourcing customer using wide area networks. The failure of a wide area network may thus make it impossible to provide the outsourced service.

Non-Existent or Insufficient Rules Regarding Information Security

Within the framework of outsourcing, outsourcing service providers receive and process large amounts of information of the outsourcing customers. Depending on the protection needs of the information to be processed, non-existent or insufficient rules may cause damage (e.g. in the event of unclear responsibilities). This is the case, for example, if the rules and instructions are not updated in the event of technical, organisational or personnel changes (e.g. when switching contact persons). The possible shortcomings in rules here ranges from ambiguities in responsibilities and control functions to rules that are incomprehensible, incoherently formulated or simply not in place.

Improper Administration of Site, System and Data Access Rights

Depending on the outsourcing project, the employees of the outsourcing customer may need site, system and data access rights for IT systems, information, buildings or rooms of the outsourcing service provider. If the processes of granting, administering and controlling these rights are specified poorly by the outsourcing service provider, this may result in extensive security issues. If the processes for granting rights are too complex, it may take too long until the employees of the outsourcing customer are granted the urgently needed rights. If the IT Operation Department provides clients with too many rights, they might access areas of other clients as a consequence.

Non-Existent or Inadequate Testing and Approval Procedures

If an outsourcing service provider has not established sufficient testing and approval procedures for the hardware and software for which they are responsible, it represents a significant threat to IT operations. Existing errors in the hardware and software or security gaps in the configuration might not be detected too late (or not at all). If new components are integrated into the operating environment without being tested sufficiently beforehand, this may also result errors or vulnerabilities from one client area also having negative effects on other customers.

If inadequate testing and approval procedures lead to security incidents, the protection required for the customer's data is no longer guaranteed. Penalties may be imposed or contracts terminated, which may have financial consequences.

Insecure Transport of Files and Storage Media

Outsourcing service providers often process large amounts of data of the outsourcing organisation. If the transport of files, documents and storage media is not sufficiently secured ac-

According to the protection needs of the information to be transported, any loss, unauthorised reading or manipulation may result in significant damage to the outsourcing organisation, but also to the outsourcing service provider. This may cause significant issues in the outsourcing business relationship. Damage may occur if files or storage media are transported to the outsourcing customer using insecure channels and these are intercepted, manipulated or lost along the way.

Insufficient Information Security Management by the Outsourcing Service Provider

Insufficiently established or inappropriately implemented information security management on the part of the outsourcing service provider entails significant risks. The problems range from a lack of overall responsibility for information security to a lack of support from the top management, insufficient strategic and conceptual specifications and a non-transparent security process. Outsourcing service providers then face the risk that the requirements of the outsourcing organisation will not be met if the overall organisation is inadequate in terms of information security.

Unsatisfactory Contractual Arrangements with an Outsourcing Customer

Due to unsatisfactory contractual arrangements, an outsourcing service provider may not provide a service in the manner required to maintain the level of security of the customer. If the protection needs and the resulting requirements regarding the security of outsourced data or systems are not known to the outsourcing service provider, they cannot be protected appropriately.

Insufficient Terms for the End of an Outsourcing Project

Without sufficient and appropriate regulations regarding the termination of the outsourcing contract, there is the risk that the business relationship will not be dissolved without conflicts. It may thus be the case that information of the customer is deleted irrevocably by the outsourcing service provider prior to this information being transmitted completely and properly to the customer. If information of the customer is deleted prematurely and completely, this may result in financial penalties for the service provider.

Inadequate Contingency Planning Concept for Outsourcing

If an outsourcing service provider has an inadequate contingency planning concept, the contractually agreed IT systems and applications might only be available a limited extent (or not at all) in an emergency. As a result, the business processes based on these systems and applications may not be available and the contractually agreed services may not be provided.

Failure of an Outsourcing Service Provider's Systems

With an outsourcing service provider, the IT systems and processes operated might fail partially or completely, which also has an impact on the outsourcing customer. If there is insufficient client separation, the failure of a system not assigned to the outsourcing customer may, under some circumstances, result in the outsourcing customer no longer being able to use the contractually stipulated service. Similar problems arise when the connection between the outsourcing service provider and customer fails.

For the outsourcing service provider, this may result in damages being claimed by the outsourcing customer based on the contract at hand.

Vulnerabilities in the Connection to an Outsourcing Service Provider

If, within the framework of an outsourcing project, the IT connection between the outsourcing service provider and the outsourcing customer is secured insufficiently, the confidentiality and integrity of the data transmitted may be endangered. However, open or poorly secured interfaces might also result in unauthorised access options for third parties regarding the systems of the organisations involved.

Social Engineering

Social engineering is a method used to gain unauthorised access to information or IT systems by "listening in" on employees. It can be used to manipulate employees into performing unauthorised tasks. Employees of outsourcing service providers may be a particularly worthwhile target in this regard because they have access to a wealth of data of different companies.

Lack of Multi-Client Capability with the Outsourcing Service Provider

Outsourcing service providers normally have numerous different customers that rely on the same resource base (IT systems, networks, personnel). If the IT systems and data of the different customers are not separated with a sufficient level of security, there is the risk that a customer may access the area of another customer. Furthermore, there might be conflicts of interest on part of the outsourcing customer if the service provider must meet comparable resource requirements simultaneously. If the respective customers are in a competitive situation, this may be particularly problematic.

Requirements

The specific requirements of module OPS.3.1 *Outsourcing for Service Providers* are listed below. As a matter of principle, the Head of IT is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. In addition, there can be other roles which have further responsibilities in implementing requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of IT
Further Roles	Head of Personnel, Data Protection Officer, BCM Officer, IT Operation Department, Top Management, Head of Organisation, Change Manager

Basic Requirements

For module OPS.3.1 *Outsourcing for Service Providers*, the following requirements **MUST** be implemented as a matter of priority:

OPS.3.1.A1 Drawing Up a Rough Concept for the Outsourcing Service

A rough concept for the outsourcing service offered **MUST** be drawn up. This rough concept **MUST** take into consideration framework conditions of outsourcing (e.g. specific requests) and address basic questions regarding the level of security and the security requirements of the outsourcing customer.

Standard Requirements

For module OPS.3.1 *Outsourcing for Service Providers*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

OPS.3.1.A2 Contractual Arrangements with Outsourcing Customers

All aspects of the outsourcing project SHOULD be stipulated in writing with the outsourcing customer in order to be able to perform the contract as requested and guarantee the required level of security. All responsibilities and duties to collaborate on creating, reviewing and changing these aspects (e.g. persons) SHOULD be specified within the framework of the agreement or also directly in the security concept between the outsourcing service provider and the outsourcing customer.

OPS.3.1.A3 Creating a Security Concept for the Outsourcing Project

The outsourcing service provider SHOULD have a security concept for its services. For individual outsourcing projects, it SHOULD also draw up specific security concepts based on the related security requirements of the outsourcing customer. Common security objectives and a joint classification for all sensitive information SHOULD be developed between the outsourcing service provider and customer. The implementation of the security concept SHOULD be checked at regular intervals.

OPS.3.1.A4 Definition of Possible Communication Partners [Head of Organisation, Data Protection Officer]

Between the outsourcing service provider and customer, it SHOULD be defined which internal and external communication partners may transmit and receive which information on the respective outsourcing project. It SHOULD be checked at regular intervals whether the communication partners are still working in their respective roles. The authorisations SHOULD be adapted in the event of changes. Between the outsourcing partners, criteria regarding which communication partners may receive which information SHOULD be specified.

OPS.3.1.A5 Provisions for Deploying the Personnel of Outsourcing Service Providers [Head of Personnel]

Employees of the outsourcing service provider SHOULD be instructed regarding their tasks and informed of existing information security regulations of the outsourcing customer in a controlled manner. If required, the employees SHOULD be vetted according to the customer's specifications (e.g. based on certificates of good conduct). The employees of the outsourcing service provider SHOULD be obliged in writing to comply with the relevant laws, regulations, non-disclosure agreements and internal provisions. Stand-in arrangements SHOULD be implemented in all areas.

OPS.3.1.A6 Procedures Regarding the Use of Third-Party Personnel [Head of Personnel]

If the outsourcing service provider deploys external personnel, the outsourcing customer SHOULD be informed accordingly. External employees performing work related to the outsourcing project SHOULD be obliged in writing to comply with the relevant laws, regulations, and internal provisions. They SHOULD be instructed regarding their tasks and, in particular, the security specifications. Third-party personnel deployed on short notice (or only once) SHOULD be treated as visitors. However, the customer's safety specifications SHOULD also be taken into account for third-party personnel.

OPS.3.1.A7 Creation of a Client Concept by an Outsourcing Service Provider

By means of an appropriate client concept, it SHOULD be ensured that the application and data contexts of different customers are separated appropriately. The client concept SHOULD be drawn up by the outsourcing service provider and made available to the outsourcing customer. The client concept SHOULD provide sufficient security for the protection needs of the outsourcing customer. The necessary client separation mechanisms SHOULD be implemented sufficiently by the outsourcing service provider.

OPS.3.1.A8 Agreement on the Connection to Networks of the Outsourcing Partners

Prior to connecting a proprietary network to the network of the outsourcing service provider, all security-relevant aspects SHOULD be specified in writing in an agreement. It SHOULD be defined who is allowed to access what areas and services of the respective other network from their own network. Contact partners SHOULD be appointed on both sides for organisational and technical questions regarding the network connection. All security gaps identified SHOULD be eliminated and the required level of security SHOULD be verifiably achieved before the network connection is activated. In the event of security issues on one or both sides, it SHOULD be specified who must be informed and what escalation steps are to be initiated.

OPS.3.1.A9 Agreement on the Exchange of Data Between the Outsourcing Partners

The required security safeguards SHOULD be agreed for the regular exchange of data among fixed communication partners of the outsourcing partners. Data formats and a secure form of data exchange SHOULD be defined. Contact partners SHOULD be appointed for both organisational and technical problems, and especially for security-related events when exchanging data with third parties. Availabilities and response times when exchanging data with third parties SHOULD be agreed. It SHOULD be defined which exchanged data may be used for what purposes.

OPS.3.1.A10 Planning and Continuity of Information Security During Ongoing Outsourcing Operations

The outsourcing customer SHOULD draw up an operating concept that takes into consideration all the relevant security aspects. The security concepts of the outsourcing partners SHOULD be checked for currency and consistency at regular intervals. The status of the security safeguards agreed SHOULD be checked at regular intervals. Regular communications, including coordination regarding changes and improvements, SHOULD be performed between the outsourcing partners.

The outsourcing partners SHOULD perform regular joint drills and tests to maintain the level of security. Information on security risks and how they are to be handled SHOULD be exchanged between the outsourcing partners at regular intervals. There SHOULD be a process that secures the flow of information when handling security incidents concerning the respective contractual partners.

OPS.3.1.A11 Site, System and Data Access Control [Head of Organisation]

Site, system and data access authorisations SHOULD be specified for the personnel of both the outsourcing service provider and the outsourcing customer. It SHOULD also be specified which authorisations are to be granted to auditors and other revisors. Only as many rights as are necessary to perform the corresponding tasks SHOULD be granted. There SHOULD be a controlled procedure for granting, managing and withdrawing authorisations.

OPS.3.1.A12 Change Management [IT Operation Department, Change Manager]

There SHOULD be policies for performing changes to IT components, software and configuration data. There SHOULD be rules specifying that security aspects must be taken into account when performing changes. All changes SHOULD be planned, tested, approved and documented. The type and extent of the documentation of changes SHOULD be coordinated with and made available to the outsourcing customer. Fallback solutions SHOULD be developed before changes are performed. In the event of major security-relevant changes, the information security management of the outsourcing organisation SHOULD already be involved in advance.

OPS.3.1.A13 Secure Migration in Outsourcing Projects

A security management team consisting of qualified employees of the outsourcing customer and the outsourcing service provider SHOULD be established for the migration phase. A security concept SHOULD be drawn up for the migration phase. Upon completion of the migration, the security concept SHOULD be updated. It SHOULD be ensured that all exceptions are reversed at the end of the migration phase. In the event of changes during the migration phase, the extent to which there is a need for adaptation to the contractual bases and existing documents SHOULD be checked.

OPS.3.1.A14 Contingency Planning for Outsourcing [BCM Officer]

A contingency planning concept for outsourcing SHOULD exist that comprises the components of the outsourcing customer and the outsourcing service provider, as well as the associated interfaces. The contingency planning concept for outsourcing SHOULD specify the responsibilities, contact persons and processes between the outsourcing customer and the outsourcing service provider. To this end, the outsourcing customer and outsourcing service provider SHOULD perform emergency drills together at regular intervals.

OPS.3.1.A15 Organised Termination of an Outsourcing Relationship [Top Management]

It SHOULD be ensured that a termination of the contractual relationship with the outsourcing customer will not impair the outsourcing customer's business activities or one's own. The outsourcing contract with the outsourcing customer SHOULD specify all aspects regarding the termination of the service relationship regardless of whether said termination is planned. The outsourcing service provider SHOULD return all the information and data of the outsourcing customer. The outsourcing service provider SHOULD then securely delete all data belonging to the customer. All authorisations configured within the framework of the outsourcing project SHOULD be reviewed and deleted if required.

Requirement in Case of Increased Protection Needs

Generic suggestions for module OPS.3.1 *Outsourcing for Service Providers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

OPS.3.1.A16 Security Vetting of Employees [Head of Personnel] (CI)

The trustworthiness of the outsourcing service provider's new employees and external personnel SHOULD be checked with the help of appropriate certificates. To this end, criteria SHOULD be contractually stipulated with the outsourcing customer.

Additional Information

For more information about threats and security safeguards for module OPS.3.1 *Outsourcing for Service Providers*, see the following publications, among others:

[27001A15]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - requirements, in particular Annex A, A.15 Supplier relationships, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[BVIT2005]	Leitfaden Business Process Outsourcing: BPO als Chance für den Standort Deutschland, [Business Process Outsourcing Guide: BPO as an Opportunity for Germany as a Business Location], Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Federal Association for Information Technology, Telecommunications and New Media) (Bitkom), Version 10.1, September 2005, https://www.bitkom.org/Bitkom/Publikationen/Leitfaden-Business-Process-Outsourcing.html , last accessed on 26.07.2018
[BVIT2008]	Leitfaden Rechtliche Aspekte von Outsourcing in der Praxis [Guide, Legal Aspects of Outsourcing in Practice]: Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (Federal Association for Information Technology, Telecommunications and New Media) (Bitkom), January 2008, https://www.bitkom.org/Bitkom/Publikationen/Rechtliche-Aspekte-von-Outsourcing-in-der-Praxis.html , last accessed on 26.07.2018
[DIN37500]	DIN ISO 37500:2015-08 Guidance on Outsourcing: August 2015
[ISFSC1.2]	The Standard of Good Practice for Information Security: Area SC1.2 Outsourcing, Information Security Forum (ISF), June 2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 15.11.2017

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module OPS.3.1 *Outsourcing for Service Providers*:

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.33 Shortage of Personnel

G 0.38 Misuse of Personal Information

G 0.41 Sabotage

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.9	G 0.14	G 0.17	G 0.18	G 0.19	G 0.22	G 0.25	G 0.30	G 0.33	G 0.38	G 0.41	G 0.45	G 0.46
OPS.3.1.A1				X									
OPS.3.1.A2							X	X	X				
OPS.3.1.A3					X							X	X
OPS.3.1.A4		X			X								X
OPS.3.1.A5								X	X				
OPS.3.1.A6								X	X				
OPS.3.1.A7					X								X
OPS.3.1.A8	X	X										X	
OPS.3.1.A9		X	X		X	X				X			X
OPS.3.1.A10					X								X
OPS.3.1.A11				X	X			X					
OPS.3.1.A12				X	X			X					
OPS.3.1.A13					X							X	X
OPS.3.1.A14	X						X		X			X	
OPS.3.1.A15					X							X	X
OPS.3.1.A16											X		



DER.1: Detecting Security-Relevant Events

Description

Introduction

In order to be able to protect IT systems, security-relevant events must be detected and handled in good time. For this, organisations must plan, implement and regularly drill appropriate organisational, personnel and technical safeguards in advance. If building on a defined and tested method is possible, reaction times can be shortened and existing processes can be optimised.

The term "security-relevant event" refers to an event that affects information security and may impair confidentiality, integrity and availability. Typical consequences of such events include information that is intercepted, manipulated, or destroyed. The causes are manifold: malware, outdated system infrastructures or internal attackers are just a few. However, attackers often exploit zero-day exploits – that is, vulnerabilities in programs that have not yet been patched. Another threat to be taken seriously involves Advanced Persistent Threats (APTs). These are targeted cyber attacks on select organisations and institutions in which an attacker gains permanent access to a network and extends this access to other systems. The attacks, which are often difficult to detect, are characterised by the very large amount of resources used and significant technical skills on the part of the attackers.

Objective

This module shows a systematic way in which information may be collected, correlated and evaluated in order to detect security-relevant events as completely and promptly as possible. The findings gained within the framework of detection are intended to improve organisations' abilities to detect and react appropriately to security-relevant events.

Not in Scope

This module includes basic requirements that must be considered and fulfilled when security-relevant events are detected. These requirements, however, are dependent upon comprehensive logging. The modules necessary in this regard are not described in the present module, but are included in OPS.1.1.5 *Logging*.

Furthermore, this module does not describe how to handle security-relevant events after they have been detected. Recommendations are also listed in DER.2.1 *Security Incident Handling* and DER.2.2 *Provisions for IT Forensics*. The module does not address the subjects of data protection or archiving logged data; these are addressed in CON.2 *Data Protection* and OPS.1.2.2 *Archiving*.

In order to detect security-relevant events, additional programs are often required, such as anti-virus programs, firewalls, or intrusion detection/prevention systems (IDS/IPS). Security aspects of these systems are also not part of the present module. They are addressed, for example, in NET.3.4 *IDS/IPS*, OPS.1.1.4 *Protection Against Malware* and NET.3.2 *Firewall*.

Threat Landscape

For module DER.1 *Detecting Security-Relevant Events*, the following specific threats and vulnerabilities are of particular importance:

Misuse of Statutory Provisions and Occupational Rights of Co-Determination

Programs detecting security-relevant events and evaluating logged data often collect a wealth of information on the network structure and the internal processes of an organisation. For example, this may include sensitive data such as personal data, confidential information, or employee workflows. Due to the fact that such data can be stored, however, employees' personal rights and rights of co-determination may be violated. Under certain conditions, the organisation may also be in violation of the respective state data protection laws or the Federal Data Protection Act.

Insufficient Qualification of Persons in Charge

During day-to-day operations of an organisation, many failures and errors may occur (e.g. a strong increase in incoming logged data). If the employees responsible have not been subject to sufficient awareness-raising and training measures, there is the risk that they will not identify security-relevant events and allow an attack to remain unnoticed.

Non-Existent or Insufficient Logging

If security-relevant events are not logged sufficiently (or at all), it will not be possible to sufficiently determine whether security provisions have been violated or attacks have been attempted with the necessary speed. In the event of damage, it will also not be possible to perform an error analysis, and the entry point used for an attack may persist as a consequence. Logged information is also used in order to perform integrity checks. However, if there are no logs, this is not possible.

Improper Administration of the Detection Systems Used

Incorrect configurations may cause the detection systems used to not work properly. For example, if the alarm settings are incorrect, the number of false alarms may increase. The employees responsible may thus no longer be able to differentiate between a false alarm and a security-relevant event. Furthermore, they might not notice messages in a timely fashion because too many alarms are being generated. As a consequence, attacks might remain unnoticed. The time required to analyse all the messages will also increase significantly.

Lack of Information Regarding the Information Domain to Be Protected

If there is insufficient information (or none at all) regarding the information domain, there is the risk that essential areas of the information domain will not be protected sufficiently by detection systems. As a consequence, attackers might easily penetrate the organisation's network and access sensitive information, for example. They may also stay in the system for extended periods of time and may access the network without this being noticed.

Insufficient Use of Detection Systems

If no detection systems are being used and the features available in IT systems and applications for detecting security-relevant events are not used either, attackers may penetrate the network of the organisation more easily without this being noticed and may access sensitive information without authorisation. Insufficient monitoring of the boundaries between networks is particularly critical.

Insufficient Personnel Resources

If the personnel available is insufficient to analyse the logged data, security-relevant events may not be detected completely. As a consequence, attacks may remain unnoticed for extended periods of time or only be detected if a large amount of sensitive information has already leaked, for example. If no external sources of information are analysed due to a shortage of personnel, vulnerabilities may also remain open for too long and may be exploited by attackers in order to illegally penetrate the IT systems of the organisation.

Requirements

The specific requirements of the module DER.1 *Detecting Security-Relevant Events* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO), User, Process Owner, Head of IT, Supervisor

Basic Requirements

For module DER.1 *Detecting Security-Relevant Events*, the following requirements **MUST** be implemented as a matter of priority:

DER.1.A1 Creation of a Security Policy for the Detection of Security-Relevant Events [Chief Information Security Officer (CISO)]

Based on the general security policy of the organisation, a specific security policy **MUST** be drawn up that transparently describes the requirements and specifications on how to plan, design and securely operate the detection of security-relevant events. The policy **MUST** be known to all employees responsible in the field of detection and **MUST** be the basis of their work. If the policy is changed or there are deviations from the requirements, this **MUST** be coordinated with the CISO responsible and documented. The correct implementation of the policy **MUST** be regularly reviewed. The results **MUST** be documented in an appropriate manner.

DER.1.A2 Compliance with Legal Conditions When Analysing Logged Data [Chief Information Security Officer (CISO)]

When analysing logged data, the legal provisions from the current federal and state laws on data protection **MUST** be followed. Furthermore, the personal rights and/or rights of co-determination of the Employee Representatives **MUST** be protected when using detection systems. It **MUST** also be ensured that all additional relevant legal provisions are taken into consideration, such as the German Teleservices Act (TMG), the German Works Constitution Act and the German Telecommunications Act.

DER.1.A3 Definition of Reporting Paths for Security-Relevant Events

Appropriate channels for reports and alerts **MUST** be defined and documented. In doing so, it **MUST** be determined which bodies must be informed at which point in time. It **MUST** also be specified how the respective persons can be reached. Depending on the urgency, a security-relevant event **MUST** be reported using different communication channels.

The employees **MUST** be provided with print-outs of the channels for reports and alerts. All persons relevant with regard to reporting and alarming **MUST** be informed of their tasks. All steps of the reporting and alerting process **MUST** be described in detail. The established channels for reports and alerts **SHOULD** be reviewed, tested and, if required, updated at regular intervals.

DER.1.A4 Raising Employee Awareness [Supervisor, Head of IT, User]

In order to enable the employees to quickly recognise security incidents, their corresponding awareness **MUST** be raised. To this end, regular training measures **SHOULD** be performed in which common and current basic threats and the approaches of cyber criminals are illustrated.

Employees' awareness **MUST** also be raised such that they will not simply ignore or close client event messages, but forward the messages to the responsible incident management using the alarm channels (see DER.2.1 *Security Incident Handling*).

Every employee **MUST** immediately report a security incident they have detected to the incident management.

DER.1.A5 Use of Provided System Features for Detection [Process Owner]

If IT systems or applications have features that can be used to detect security-relevant events, these **MUST** be enabled and used.

Logging **MUST** be enabled on all components used (see OPS.1.1.5 *Logging*). In the event of a security-relevant incident, the messages **MUST** at least be analysed locally. The logged events of other IT systems **MUST** be checked, as well. In addition, the collected messages **SHOULD** be checked randomly at intervals defined in a binding manner.

It **MUST** be checked whether additional malicious code scanners should be installed on central IT systems (see also SYS.1.1 *General Server*). If this is the case, the scanners **MUST** make it possible to analyse their messages and logs via a central means of access. In addition, they **MUST** be updated regularly. It **MUST** be ensured that the malicious code scanners automatically report security-relevant events to the persons in charge and that the messages are actually analysed and investigated.

Standard Requirements

For module DER.1 *Detecting Security-Relevant Events*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

DER.1.A6 Continuous Monitoring and Analysis of Logged Data [User]

All logged data SHOULD be actively monitored and analysed as constantly as possible. Responsible employees SHOULD be made responsible for these activities.

If the employees responsible have to actively search for security-relevant events that have occurred (e.g. when testing or monitoring IT systems), such tasks SHOULD be documented in corresponding procedural instructions.

Sufficient personnel resources SHOULD be made available for detecting security-relevant events.

DER.1.A7 Training Persons in Charge [Supervisor, Head of IT]

All persons in charge of reviewing event messages SHOULD be subjected to advanced training and qualification measures. When IT components are procured, a budget for training measures SHOULD be factored in and a training concept SHOULD be drawn up for the employees responsible.

DER.1.A8 Definition of Segments to Be Protected [Process Owner]

Based on the network plan (see NET.1.1 *Network Architecture and Design*), it SHOULD be defined which network segments must be protected by additional detection systems (cf. DER.1.A9 *Use of Additional Detection Systems*).

DER.1.A9 Use of Additional Detection Systems [Process Owner]

In order to better detect security-relevant events, the information domain SHOULD be complemented by additional detection systems and sensors. Malicious code detection systems SHOULD be used and administered from a central location. The transitions defined in the network plan between internal and external networks SHOULD be complemented by network-based intrusion detection systems (NIDS).

DER.1.A10 Use of TLS/SSH Proxies [Process Owner]

At the transitions to external networks, TLS/SSH proxies SHOULD be used that interrupt encrypted connections and thereby make it possible to check the data transmitted for malware. All TLS/SSH proxies SHOULD be protected against unauthorised access. Furthermore, security-relevant events on the TLS/SSH proxies SHOULD be detected automatically. An organisational rule SHOULD be drawn up that specifies how logged data can be evaluated manually in accordance with the provisions of data protection law.

DER.1.A11 Use of a Central Logging Infrastructure to Evaluate Security-Relevant Events [Process Owner]

The event messages collected by the IT systems and application systems SHOULD be stored in a centralised log infrastructure (see OPS1.1.5 *Logging*). It SHOULD be possible to store, evaluate and retrieve the event messages provided in a centralised manner using a tool. In order to be able to correlate and compare the data, it SHOULD be synchronised in terms of time. The collected event messages SHOULD be checked for particularities at regular intervals. In order to

be able to detect security-relevant events retrospectively, as well, the signatures of the detection systems SHOULD all be up to date and have the same status.

DER.1.A12 Evaluation of Information from External Sources [Chief Information Security Officer (CISO), Process Owner]

In order to obtain new findings regarding security-relevant events for one's own information domain, external sources SHOULD be used and evaluated. Since messages are received by an organisation via different channels, it SHOULD be ensured that these messages are actually identified as relevant by the employees and forwarded to the proper recipient. If information comes from qualified sources, it SHOULD be evaluated as a matter of principle. All information received SHOULD be evaluated as to whether it is relevant for one's own information domain. If this is the case, the information SHOULD be escalated according to security incident handling (see DER.2.1. *Security Incident Handling*).

DER.1.A13 Regular Audits of Detection Systems

The existing detection systems and implemented safeguards SHOULD be audited regularly as to whether they are still up to date and effective. The measures evaluated SHOULD include those that accrue when security-relevant events are recorded, reported and escalated (for example). The audit results SHOULD be documented comprehensibly and compared to the target condition. Deviations SHOULD be investigated.

Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.1 *Detecting Security-Relevant Events* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

DER.1.A14 Evaluation of Logged Data by Specialised Personnel [Head of IT] (CI)

Employees SHOULD be mainly assigned to monitor all types of logged data. The deployed personnel SHOULD be subjected to specialised advanced training and qualification measures. A group of persons SHOULD be appointed that will only be responsible for the subject of evaluating logged data (e.g. from the field of forensics).

DER.1.A15 Central Detection and Real-Time Examination of Event Messages (CIA)

Central components SHOULD be used in order to detect and evaluate security-relevant events. Central automated analyses performed by software SHOULD be used in order to record all events occurring in the system environment, compare these to one another, and make security-relevant processes visible. It SHOULD be possible to view and evaluate all data received in the log administration in a seamless manner. The actual data SHOULD be analysed as constantly as possible. If defined threshold values are exceeded, an alarm SHOULD be generated automatically. The personnel SHOULD make sure that a qualified reaction corresponding to the requirements is initiated immediately in the event of an alarm. In this context, the employee concerned SHOULD also be informed immediately.

The persons in charge of the system SHOULD audit and, if required, adapt the analysis parameters at regular intervals. In addition, data that has already been audited SHOULD be examined automatically for security-relevant events at regular intervals.

DER.1.A16 Use of Detection Systems in Accordance with Protection Requirements (CIA)

Applications with higher protection needs SHOULD be protected by means of additional detection measures. For this, detection systems SHOULD be used that also make it possible to guarantee higher protection needs in technical terms.

DER.1.A17 Automatic Reaction to Security-Relevant Events (CI)

In the event of a security-relevant event, the detection systems used SHOULD automatically report the event and react by employing appropriate security safeguards. In the process, methods SHOULD be used that automatically detect possible attacks, misuse attempts, or security violations. It SHOULD be possible to automatically intervene in data flows in order to prevent a possible security incident.

DER.1.A18 Performance of Regular Integrity Checks (CI)

All detection systems SHOULD be checked regularly as to whether their integrity is still intact. The user rights SHOULD also be checked. In addition, the sensors SHOULD perform an integrity check on files and trigger an automatic alarm in the event of changing values.

Additional Information

For more information about threats and security safeguards for module DER.1 *Detecting Security-Relevant Events*, see the following publications, among others:

[BSILeit1]	BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen [BSI Guideline on Introducing Intrusion Detection Systems]: Version 1.0, October 2002, https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/index_hm.html , last accessed on 05.10.2018
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 15.11.2017

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module DER.1 *Detecting Security-Relevant Events*:

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.33 Shortage of Personnel
- G 0.37 Repudiation of Actions
- G 0.38 Misuse of Personal Information
- G 0.39 Malware
- G 0.40 Denial of Service
- G 0.41 Sabotage
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0. 9	G 0. 11	G 0. 18	G 0. 19	G 0. 20	G 0. 21	G 0. 22	G 0. 23	G 0. 25	G 0. 26	G 0. 27	G 0. 28	G 0. 29	G 0. 30	G 0. 31	G 0. 32	G 0. 33	G 0. 37	G 0. 38	G 0. 39	G 0. 40	G 0. 41	G 0. 46
DER.1.A1			X								X												
DER.1.A2				X									X					X	X				
DER.1.A3			X														X						
DER.1.A4			X							X					X								
DER.1.A5	X					X	X	X				X		X	X	X				X		X	
DER.1.A6			X					X	X	X	X			X		X				X			
DER.1.A7			X												X	X							
DER.1.A8	X		X																				
DER.1.A9	X					X		X						X	X	X				X		X	
DER.1.A10						X		X					X			X				X			
DER.1.A11	X			X		X		X	X	X	X	X		X	X	X			X		X		
DER.1.A12					X							X											
DER.1.A13			X	X	X	X	X	X		X	X			X		X				X			
DER.1.A14		X									X						X						
DER.1.A15	X			X		X		X	X	X	X	X		X	X	X			X		X		X
DER.1.A16			X			X		X						X		X					X	X	X
DER.1.A17	X							X			X	X		X		X				X	X		



DER.2.1: Security Incident Handling

Description

Introduction

In order to limit damage and avoid additional damage, detected security incidents need to be processed quickly and efficiently. To this end, it is necessary to establish a specified and tested method for handling security incidents (also referred to as *security incident handling* or *security incident response*).

A security incident may have significant effects on an organisation and entail major damage. Examples of such incidents include incorrect configurations that cause confidential information to be disclosed, or criminal acts such as the hacking of servers, the theft of confidential information, sabotage, or blackmail associated with IT.

The causes of security incidents are manifold: malware, outdated system infrastructures or internal attackers are just a few. However, attackers also often exploit zero-day exploits. Another threat to be taken seriously involves Advanced Persistent Threats (APTs).

Furthermore, users, administrators, or external service providers may behave inappropriately, such as by changing system parameters in a security-critical manner or violating internal policies. In addition, plausible causes include violations of access rights, changes in software or hardware, or insufficient protection of sensitive rooms and buildings.

Objective

The objective of this module is to show a systematic way to draw up a concept for security incident handling.

Not in Scope

This module focuses on handling security incidents from the standpoint of information technology. Before security incidents can be handled, however, they must first be detected. Security requirements in this regard are included in module DER.1 *Detecting Security-Relevant Events*; they are a prerequisite of the present module. The initial forensic examination is addressed in module DER.2.2 *Provisions for IT Forensics*, and cleaning after an APT incident is addressed in module DER.2.3 *Clean-Up of Extensive Security Incidents*. A special area of handling security incidents is business continuity management, which is addressed in the module DER.4 *Business Continuity Management* and not considered further here. However, it must be considered that the decision as to whether there is an emergency or not is made in the present module.

Threat Landscape

For module DER.2.1 *Security Incident Handling*, the following specific threats and vulnerabilities are of particular importance:

Inappropriate Handling of Security Incidents

In practice, it is impossible to completely eliminate the possibility of security incidents occurring. This is also true when numerous security safeguards have been implemented. If there is an inappropriate response to acute security incidents (or none at all), this may result in major (or even catastrophic) damage. Examples include:

- Suspicious entries being found in the log files of a firewall. If it is not examined promptly whether this is the first sign of a possible attempt to penetrate the system, attackers may successfully attack and overcome the firewall without being noticed and penetrate the internal network of the organisation.
- The presence of vulnerabilities in the IT systems and applications used is announced. If this information is not obtained in good time and the necessary countermeasures are not initiated and implemented quickly, attackers may exploit the corresponding vulnerabilities.

Bad and hasty decisions may be made under stress when there is no appropriate approach prescribed for handling security incidents. For example, these decisions may result in the press being informed incorrectly and a negative public image being created as a consequence, third parties incurring losses due to their own IT systems and demanding compensation, or no alternative or recovery safeguards being provided, which can significantly increase the damage sustained by the organisation.

Undetected Security Incidents

During day-to-day operations of an organisation, many failures and errors may occur. In this context, security incidents may not be identified as such by personnel and an attack (or a related attempt) may remain undetected. Even if the employees have been adequately trained and their awareness has been raised regarding the issues relating to information security, it cannot be ruled out that they may fail to recognise security incidents. Examples of this include:

- A user who has not logged into the local network of their organisation for a long time assumes that the extremely slow response of their laptop when accessing the Internet, which they noticed over a week ago, is normal and fails to notice that a malicious program is active in the background. They were not (or insufficiently) trained to inform the person responsible for security after noticing suspicious activities.
- A production manager does not notice that data in the production systems and also the control display systems has been changed in a covert manner. They do not suspect anything when the SCADA controller of the production system displays unusual values because this only happens for a short period of time. The incident is not reported because all values have returned to the expected display values. As a consequence, no one notices that the display values were manipulated by malware.
- A burglary in a branch office of a company is assumed to be a case of drug-related crime because laptops and flat-screen monitors were the only objects stolen. The fact that confidential information and access data for IT systems in the intranet were stored on the laptops is

not considered to be important, and the CISO is not informed. For this reason, the organisation is not prepared for the subsequent attacks on the IT systems at the company's other locations and at its headquarters. The data found on the stolen laptops is used for the attack.

Destruction of Evidence While Handling Security Incidents

When the action taken to handle a security incident is performed carelessly or the applicable specifications are disregarded, important evidence needed to investigate the incident or pursue legal action may be unintentionally destroyed or rendered inappropriate for court proceedings.

Examples of this include:

- An attacker infects a personal computer with malware whose mode of operation and objective may only be analysed when the system is running. For this, information on the active processes and the content of the main memory must be backed up and evaluated. If the personal computer is shut down prematurely, the information pertaining to when the system was running can no longer be used to analyse and clarify the security incident.
- An administrator finds a running process on a server that is causing an extraordinary CPU load. In addition, this process is creating temporary files and sending unknown information over the Internet. If the process is terminated prematurely and the temporary files are simply deleted, it will not be possible to find out whether the theft of confidential information was successful.
- An important server becomes compromised because the administrator was not able to install the latest security updates as planned due to the heavy load on the server and the lack of a free maintenance window. To avoid any possible disciplinary consequences, the administrator installs the missing updates before a security team is able to analyse the source of the intrusion and the damage resulting from it. A low tolerance for employee errors therefore prevented analysis of the problem.

Requirements

The specific requirements of module DER.2.1 *Security Incident Handling* are listed below. As a matter of principle, the Chief Information Security Officer is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Data Protection Officer, BCM Officer, IT Operation Department, Top Management, Press Office, Process Owner, Head of IT

Basic Requirements

For module DER.2.1 *Security Incident Handling*, the following requirements **MUST** be implemented as a matter of priority:

DER.2.1.A1 Definition of a Security Incident [Head of IT]

Within an organisation, the meaning of the term "security incident" **MUST** be clearly defined. A security incident **MUST** be distinguished from failures during day-to-day operations whenever possible. All employees involved in the process of handling security incidents **MUST** be familiar with the definition of a security incident. The definition and the threshold of occurrence **SHOULD** be based on the protection needs of the affected business processes, IT services, IT systems, and IT applications.

DER.2.1.A2 Drawing Up a Policy for Handling Security Incidents

A policy **MUST** be drawn up to govern the handling of security incidents. This policy **MUST** define its purpose and objective and govern all aspects of handling security incidents. Therefore, codes of conduct for the different kinds of security incidents **MUST** be described. In addition, there **MUST** be target-group-oriented and practically usable instructions for all employees. Furthermore, the interfaces with other management areas **SHOULD** be taken into account, including in business continuity management.

The policy **MUST** be known to all employees. It **MUST** be coordinated with the IT management and IT Operation Department and approved by the organisation's top management. The policy **MUST** be reviewed and updated regularly.

DER.2.1.A3 Specification of Responsibilities and Contact Persons in the Event of Security Incidents [Head of IT]

It **MUST** be specified who will be responsible for what in the event of security incidents. The tasks and competencies applicable in the event of security incidents **MUST** be defined for all employees. Employees who are to process security incidents **MUST** also be informed of their tasks and competencies. In this context, it **MUST** be specified who will make the eventual decision regarding a forensic examination, the criteria to be followed in carrying it out and when this should take place.

The employees **MUST** be familiar with the contact persons for all kinds of security incidents. Contact information **MUST** always be up to date and present in a practicable form.

DER.2.1.A4 Notification of Entities Affected by Security Incidents [Press Office, Top Management, Head of IT, Data Protection Officer, BCM Officer]

When a security incident occurs, all the internal and external entities affected **MUST** be informed of the incident promptly. In this process, it **MUST** be checked whether the Data Protection Officer, the works council/personnel council, and employees from the legal department must be consulted. The reporting duties for public authorities and regulated industries **MUST** be taken into consideration, as well. Furthermore, it **MUST** be guaranteed that the entities affected are informed of the required safeguards.

DER.2.1.A5 Remedial Action in Connection with Security Incidents [Head of IT, IT Operation Department]

In order for a security incident to be remedied successfully, the person responsible **MUST** initially contain the problem and find the cause. Afterwards, they **MUST** select the necessary re-

medial safeguards and obtain approval from the Head of IT prior to implementing them. Afterwards, the cause **MUST** be eliminated and a secure condition **MUST** be established (see DER.2.1.A6 *Recovering the Operating Environment After Security Incidents*).

There **MUST** be a current list of internal and external security experts who may be consulted in the event of security incidents to help answer questions from the various subject areas required. Secure communication methods with these internal and external entities **MUST** be established.

DER.2.1.A6 Recovering the Operating Environment After Security Incidents [Head of IT, IT Operation Department]

In order to eliminate the consequences of security incidents, the components affected **MUST** be disconnected from the network and all necessary data that could provide information on the type and cause of the problem **MUST** be backed up. On all components affected, the operating system and all applications **MUST** be checked for changes.

The original data **MUST** be re-installed from write-protected data storage media. In so doing, all security-related configurations and patches **MUST** also be implemented again. If data from backups is reimported, it **MUST** be ensured that the data was not affected by the security incident. Before restarting operations after an attack, all passwords on the components affected **MUST** be changed. The components affected **SHOULD** be subjected to a penetration test before they are used again.

When recovering the secure operating environment, the users **MUST** be involved in the functional tests of the applications. After everything has been recovered, the components (including the network transitions) **MUST** be monitored in a targeted manner in order to be able to detect further attempted attacks.

If external service providers are used in order to remedy failures, it **MUST** be specified which information on the security incident is made available to whom.

Standard Requirements

For module DER.2.1 *Security Incident Handling*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

DER.2.1.A7 Establishment of a Procedure for Handling Security Incidents

In order for organisations to respond appropriately to security incidents, an appropriate procedure for handling security incidents **SHOULD** be defined. In doing so, the procedures, processes and specifications for different security incidents **SHOULD** be stipulated unambiguously and documented appropriately. The organisation's top management **SHOULD** implement and publish the final procedure. The procedure **SHOULD** be reviewed and updated regularly.

DER.2.1.A8 Design of Organisational Structures for Handling Security Incidents

Appropriate organisational structures **SHOULD** be defined for handling security incidents. Therefore, a security incident team **SHOULD** be established with members who may be called in depending on the type of incident. Even if the security incident team only meets when a specific security incident has occurred, appropriate members **SHOULD** already be appointed in advance and instructed on how to perform their tasks. The composition of the security incident team **SHOULD** be updated at regular intervals.

DER.2.1.A9 Specification of Reporting Channels for Security Incidents [Head of IT]

For the different types of security incidents, the reporting channels appropriate in each case SHOULD be established. In so doing, it SHOULD be ensured that employees may quickly and easily report security incidents using reliable and trustworthy channels.

If a central contact point for reporting failures or security incidents is established, this SHOULD also be communicated to all employees.

There SHOULD be a communication and contact strategy. This strategy SHOULD specify who must be informed as a matter of principle, who may be informed, who is responsible for handling this and in what order, and the level of detail of the information provided. It SHOULD be specified who will pass information on security incidents on to third parties. It SHOULD also be ensured that no unauthorised persons forward information on the security incident.

DER.2.1.A10 Limiting the Effects of Security Incidents [Head of IT, BCM Officer, IT Operation Department]

During the analysis of the causes of a security incident, it SHOULD be decided whether it is more important to contain the damage occurred or to investigate it. In order to be able to estimate the effects of a security incident, sufficient information SHOULD be present. For certain security incident scenarios, worst-case considerations SHOULD already be performed in advance.

DER.2.1.A11 Classification of Security Incidents [Head of IT, IT Operation Department]

A uniform procedure SHOULD be defined for classifying security incidents and failures. The classification procedure for security incidents SHOULD be coordinated between security management and incident management.

DER.2.1.A12 Specification of Where Security Incident Handling Overlaps with Incident Management [BCM Officer]

The interfaces between incident management, business continuity management and security management SHOULD be analysed. In so doing, resources that may support joint use SHOULD be defined as well.

The employees involved in incident management SHOULD be made aware of issues in the field of handling security incidents and business continuity management. The security management SHOULD have read-only access to the incident management tools used.

DER.2.1.A13 Integration into Security and Business Continuity Management [BCM Officer]

As part of security management, handling security incidents SHOULD be specified in the security policy and security concept of the organisation. Handling security incidents SHOULD also be coordinated with business continuity management. If a special incident management role has already been established in the organisation, this person SHOULD also be involved.

DER.2.1.A14 Escalation Strategy for Security Incidents [Head of IT]

An escalation strategy SHOULD be formulated that goes beyond the communication and contact strategy (see DER.2.1.A9 *Specification of Reporting Paths for Security Incidents*). The persons responsible for incident management and information security management SHOULD work together during the development of the escalation strategy.

The escalation strategy SHOULD include clear instructions stating who needs to be involved using which reporting paths within what time frame and for which type of detected or suspected security incidents. It SHOULD also be specified which safeguards and activities will be triggered by escalation.

Suitable tools SHOULD be selected for the defined escalation strategy. These SHOULD also be appropriate for confidential information. It SHOULD be ensured that the tools will also be available during security incidents and in cases of emergency.

The escalation strategy SHOULD be reviewed and, if required, updated regularly. The checklists (matching scenarios) for incident management SHOULD be complemented by security-relevant topics and updated regularly. The defined escalation paths SHOULD be tested within the context of drills.

DER.2.1.A15 Training Employees Within the Central IT Operation Department Contact Point on Handling Security Incidents [Head of IT] (I)

The employees of the service desk SHOULD be familiar with the policies for handling security incidents. They SHOULD be provided with suitable additional resources for detecting such incidents. They SHOULD be trained sufficiently regarding their use. The employees of the service desk SHOULD be familiar with the protection needs of the systems affected. The checklists of the service desk SHOULD also include questions designed to help identify security incidents.

DER.2.1.A16 Documentation of Security Incident Handling

The process of remedying security incidents SHOULD be documented in accordance with a standardised procedure. All actions performed, including the respective times, SHOULD be documented along with the logged data of the components affected. In so doing, confidentiality SHOULD be guaranteed while documenting the information and archiving the reports.

The necessary information SHOULD be entered into the respective documentation systems before the failure is marked as finished and completed. For this, the required quality assurance requirements SHOULD be defined in advance together with security management.

DER.2.1.A17 Evaluation of Security Incidents

Security incidents SHOULD be evaluated in a standardised manner. In so doing, it SHOULD be examined how quickly security incidents were detected and remedied, whether the reporting channels worked, whether sufficient information was available for evaluation and whether the detection safeguards were effective. It SHOULD also be checked whether the implemented safeguards and activities were effective and efficient.

The experience gained from previous security incidents SHOULD be used to develop instructions for comparable security incidents. These instructions SHOULD be announced to the relevant groups of persons and updated at regular intervals on the basis of new findings.

Furthermore, top management SHOULD be informed of the security incidents at annual intervals. However, top management SHOULD be informed immediately if there is an immediate need for action.

DER.2.1.A18 Further Development of Processes Based on Findings from Security Incidents and Industry Developments [Process Owner]

The reactions to security incidents SHOULD be analysed and examined in terms of whether processes and procedures need to be changed or developed further. Both those involved in re-

actions to security incidents and those responsible SHOULD report on their respective experiences.

It SHOULD be checked whether there are new developments in the fields of incident management and forensics, and it SHOULD be possible to incorporate them into the respective documents and procedures.

If additional resources and checklists are used (e.g. for service-desk employees), it SHOULD be checked whether they need to be complemented by required questions and information.

Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.2.1 *Security Incident Handling* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

DER.2.1.A19 Specifying Priorities for Handling Security Incidents (CIA)

In order to be able to remedy the causes of security incidents and resulting damage in an efficient manner and a sensible order, the priorities SHOULD be defined in advance and updated at regular intervals. In so doing, the established classification of security incidents SHOULD also be taken into consideration (see DER.2.1.A11 *Classification of Security Incidents*).

The priorities SHOULD be approved and implemented by the organisation's top management. All decision makers involved in handling security incidents SHOULD be familiar with them. The defined priority classes SHOULD also be stored in incident management.

DER.2.1.A20 Creation of an Internal Reporting Office for Security Incidents (CIA)

An internal office for reporting security incidents SHOULD be established. It SHOULD be guaranteed that the reporting office is available during normal office hours. However, it SHOULD also be possible for employees to report security incidents outside of normal office hours. The employees of the reporting office SHOULD be adequately trained on and made aware of issues related to information security. All information on security incidents SHOULD be treated confidentially within the reporting office.

DER.2.1.A21 Assembling a Team of Experts for Handling Security Incidents (CIA)

In order to competently escort security incidents through the entire lifecycle of the security incident handling process, a team of experienced and trustworthy specialists SHOULD be assembled. Along with technical knowledge, the members of the team SHOULD also have corresponding communication skills. The trustworthiness of the members of the team of experts SHOULD be checked. The composition of the team of experts SHOULD be updated at regular intervals.

The members of the team of experts SHOULD be included in the escalation and reporting channels. The team of experts SHOULD be trained to analyse security incidents in the systems deployed in the organisation. The members of the team of experts SHOULD receive regular training on both the systems used and detecting and responding to security incidents. The team of experts SHOULD have access to any existing documentation and financial and technical resources required to handle security incidents quickly and discretely.

The team of experts SHOULD be appropriately considered and integrated in the organisational structures (see DER.2.1.A8 *Design of Organisational Structures for Handling Security Incidents*). The responsibilities of the team of experts SHOULD be coordinated in advance with those of the security incident team (see DER.2.1.A3 *Specification of Responsibilities and Contact Persons in the Event of Security Incidents*).

DER.2.1.A22 Reviewing the Management System for Handling Security Incidents (CIA)

The management system for handling security incidents SHOULD be checked regularly as to whether it is still up to date and effective. To this end, both announced and unannounced drills SHOULD be conducted. The drills SHOULD be coordinated in advance with top management. The measures accrued when recording, reporting and escalating security incidents (for example) SHOULD be evaluated.

Furthermore, simulation games for handling security incidents SHOULD be performed in order to promote the development of the necessary practical skills.

Additional Information

For more information about threats and security safeguards for module DER.2.1 *Security Incident Handling*, see the following publications, among others:

[27001A16]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management system - Requirements, especially Annex A, A.16 Information security incident management, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[27035]	ISO/IEC 27035:2016: Information technology - Security techniques - Information security incident management - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, November 2016
[ISFSATS14]	The Standard of Good Practice for Information Security : Area SA (System Access) and TS1.4 (Technical Security Management; Identity and Access Management), Information Security Forum (ISF), June 2018
[NIST80061]	Computer Security Incident Handling Guide: NIST Special Publication 800-61 Revision 2, August 2012, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf , last accessed on 05.10.2018
[NIST80083]	Guide to Malware incident Prevention and Handling for Desktops and Laptops: NIST Special Publication 800-83 Revision 1, July 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module DER.2.1 *Security Incident Handling*:

G 0.11 Failure or Disruption of Service Providers

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.11	G 0.18	G 0.19	G 0.20	G 0.22	G 0.25	G 0.27	G 0.29	G 0.30	G 0.32	G 0.33	G 0.45	G 0.46
DER.2.1.A1		X	X	X				X					
DER.2.1.A2		X					X	X					
DER.2.1.A3		X					X	X			X		
DER.2.1.A4			X	X				X					
DER.2.1.A5	X	X	X			X	X	X					
DER.2.1.A6	X	X	X			X		X	X	X		X	X
DER.2.1.A7		X					X	X					
DER.2.1.A8		X					X	X			X		
DER.2.1.A9		X	X	X	X		X	X			X		
DER.2.1.A10		X				X		X				X	X
DER.2.1.A11		X	X					X					
DER.2.1.A12		X	X				X						X
DER.2.1.A13		X											X
DER.2.1.A14		X	X	X	X			X					X
DER.2.1.A15		X	X	X				X					
DER.2.1.A16		X						X					
DER.2.1.A17		X	X	X	X			X				X	X
DER.2.1.A18		X	X	X				X				X	X
DER.2.1.A19		X				X	X				X	X	X
DER.2.1.A20		X	X	X	X		X	X		X		X	X
DER.2.1.A21		X	X	X			X	X		X	X	X	X

DER.2.1.A22	X	X	X	X	X	X	X	X			X	X	X
-------------	---	---	---	---	---	---	---	---	--	--	---	---	---



DER.2.2: Provisions for IT Forensics

Description

Introduction

IT forensics is the strictly methodical data analysis of storage media and in computer networks for the clarification of incidents.

Forensic examination of IT security incidents is always required to determine the extent of damage, thwart attacks and prevent them in the future, and identify attackers. Whether or not an IT security incident requires forensic examination is determined whilst handling the incident. In the context of this module, IT forensic examination consists of the following phases:

- **Strategic preparation:** during this phase, processes are planned and established to ensure that an organisation is able to forensically analyse IT security incidents. It is also required if the organisation does not have its own forensics experts.
- **Initialisation:** once the responsible employees have decided to forensically examine an IT security incident, the previously planned processes are started. Moreover, the examination framework is specified, and initial measures are performed.
- **Securing evidence:** here, the evidence to be secured is selected, and the data is secured forensically. In this regard, a differentiation is made between live forensics and post-mortem forensics: live forensics ensures that volatile data (e.g. network connections, RAM) of a running IT system is secured. During post-mortem forensics, forensic copies of storage media are created.
- **Analysis:** the collected data is analysed forensically. In this regard, data is considered both individually and in the overall context.
- **Presentation of results:** the relevant examination results are processed and communicated to meet the needs of specific target groups.

Objective

This module shows the safeguards required to conduct forensic IT examinations. In particular, it addresses how to make corresponding preparations and secure evidence.

If providers of forensics services secure evidence either partially or entirely on their own, such requirements also apply to them. Contractual arrangements and tests can be used to ensure that a service provider will comply with such requirements.

Not in Scope

This module does not describe requirements that are designed to ensure that attacks will be detected. These are included in module DER.1 *Detecting Security-Relevant Events* and are a prerequisite of the present module. In addition, this module does not address criteria and processes used by the persons in charge in order to decide whether an IT security incident must be forensically examined. The decision on this will be made whilst handling the security incident (see DER.2.1 *Security Incident Handling*).

Furthermore, this module only addresses safeguards that are essential for later forensic IT examinations. The actual performance of forensic analysis is thus not part of this module. The module does not cover forensic IT investigations for criminal offences or other matters of criminal relevance either.

Finally, the module does not address how IT infrastructures can be cleaned after being attacked (see DER.2.3 *Clean-Up of Extensive Security Incidents*). However, the activities described therein can be supported significantly by the results of forensic IT examinations.

Threat Landscape

For module DER.2.2 *Provisions for IT Forensics*, the following specific threats and vulnerabilities are of particular importance:

Violation of Legal Framework Conditions

In many cases, all data considered to be necessary is copied, secured and evaluated for forensic IT examinations. This typically also includes personal data of employees or partners. If such data is accessed without justification and without the involvement of the Data Protection Officer, for example, the organisation has violated related legal regulations (e.g. if there is a breach of limited use). It is also possible that the collected data can be used, for example, to derive the behaviour of employees or establish references to them. This also includes the risk that internal regulations will be violated.

Loss of Evidence Due to Incorrect or Incomplete Securing of Evidence

If evidence is secured incorrectly or too slowly, this may result in the loss of important data that cannot later be recovered. In the worst case, this will result in a forensic examination that produces no findings. At minimum, however, the value of the evidence will be limited.

The risk of losing important evidence increases significantly if employees use forensic tools incorrectly, secure data too slowly or practise too little. Evidence often gets lost if the persons in charge do not identify volatile data as relevant and thus fail to secure it.

Requirements

The specific requirements of module DER.2.2 *Provisions for IT Forensics* are listed below. As a matter of principle, the Chief Information Security Officer is responsible for fulfilling the requirements. Furthermore, the CISO is responsible for ensuring that all requirements are met

and verified according to the security concept defined. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Data Protection Officer, Top Management, Investigator, Head of Investigation

Basic Requirements

For module DER.2.2 *Provisions for IT Forensics*, the following requirements **MUST** be implemented as a matter of priority:

DER.2.2.A1 Examination of Legal and Regulatory Framework Conditions for Acquisition and Evaluation [Data Protection Officer, Top Management]

If data is acquired and evaluated for forensic examinations, all legal and regulatory framework conditions **MUST** be identified and met; see ORP.5 *Compliance Management*. Internal regulations and agreements with employees **MUST NOT** be violated. In individual cases, however, it can be necessary to weigh the interests of the organisation against the interests of the employees. In such instances, the supervisory/personnel board and the Data Protection Officer **MUST** be involved.

DER.2.2.A2 Drawing Up a Guide for Initial Measures in Case of an IT Security Incident

A guide describing the initial measures to be taken for the employed IT systems in case of an IT security incident **MUST** be drawn up in order to destroy as little evidence as possible. This **MUST** also describe the actions that could destroy potential evidence and how this can be avoided.

DER.2.2.A3 Pre-Selection of Forensic Service Providers

If an organisation does not have its own forensics team, suitable providers of forensic services **MUST** already be identified during the preparatory phase. The eligible providers of forensic services **MUST** be documented.

Standard Requirements

For module DER.2.2 *Provisions for IT Forensics*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

DER.2.2.A4 Specifying Interfaces with Crisis and Business Continuity Management

The interfaces between forensic IT examinations and crisis and business continuity management **SHOULD** be defined and documented. In this regard, it **SHOULD** be specified which employees are responsible for what actions, and how communication with them should proceed. Furthermore, it **SHOULD** be ensured that contact persons are available.

DER.2.2.A5 Drawing Up a Guide for Measures of Securing Evidence in Case of IT Security Incidents

A guide describing how to secure evidence SHOULD be drawn up. This SHOULD specify corresponding procedures, technical tools, legal framework conditions and documentation requirements.

DER.2.2.A6 Training Personnel on Forensic Securing of Evidence

All responsible employees SHOULD know how to secure evidence and use forensic tools correctly. In this regard, suitable training SHOULD be offered.

DER.2.2.A7 Selecting Forensic Tools

It SHOULD be ensured that tools for forensically securing and analysing evidence are suitable for these purposes. Before using a forensic tool, it SHOULD be checked that it works properly. It SHOULD also be verified and documented that it has not been manipulated.

DER.2.2.A8 Selection and Order of Evidence to Be Secured [Head of Investigation]

A forensic examination SHOULD always start by defining goals or with the work order in question. The goals SHOULD be formulated as precisely as possible. Then, all required data sources SHOULD be identified. The order in which data is to be secured and the detailed process for doing so SHOULD also be specified. The order SHOULD be based on the volatility of the data to be secured. Highly volatile data SHOULD be secured promptly. Only then SHOULD read-only memory and backups (for example) be secured.

DER.2.2.A9 Pre-Selection of Forensically Relevant Data [Head of Investigation]

The method and the time period for storing secondary data (e.g. log data or traffic transcripts) within the scope of the legal framework conditions for possible forensic measures of securing evidence SHOULD be specified.

DER.2.2.A10 Forensic IT Securing of Evidence [Investigator, Head of Investigation]

To secure evidence, entire storage media SHOULD be forensically duplicated whenever possible. If this is not possible (e.g. in the case of volatile data in RAM or in SAN partitions), a method that changes as little data as possible SHOULD be selected.

The original storage media SHOULD be stored in a sealed manner in order to prove that the integrity of the data is still intact. If cryptographic checksums of forensic copies or original copies exist, they can also be used to prove integrity. To this end, several copies of the cryptographic checksums documented in writing SHOULD be stored separately from the storage media. In addition, it SHOULD be ensured that the checksums documented in this way cannot be changed. A witness SHOULD confirm the corresponding procedure and certify the checksums so that the data is admissible in court.

Only trained personnel (see DER.2.2.A6 *Training Personnel on Forensic Securing of Evidence*) or a provider of forensic services (see DER.2.2.A3 *Pre-Selection of Forensic Service Providers*) SHOULD be assigned to secure evidence.

DER.2.2.A11 Documentation of Securing Evidence [Investigator, Head of Investigation]

When evidence is secured forensically, all the steps required SHOULD be documented. The documentation SHOULD provide seamless proof of how secured original evidence has been handled. In addition, the employed methods and the reasons why the persons in charge used them SHOULD be documented.

DER.2.2.A12 Secure Storage of Original Storage Media and Evidence [Investigator, Head of Investigation]

All secured original storage media SHOULD be stored physically so that only investigating employees known by name can access them. If original storage media and evidence are stored, the storage period SHOULD be specified. After this period expires, it SHOULD be checked whether the storage media and evidence must be stored further. After the end of the storage period, evidence SHOULD be securely deleted or destroyed, and original storage media SHOULD be returned.

Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.2.2 *Provisions for IT Forensics* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

DER.2.2.A13 Framework Agreements with External Service Providers (CIA)

The organisation SHOULD entered into call-in agreements or framework agreements with providers of forensic services so that IT security incidents can be forensically examined more quickly.

DER.2.2.A14 Specifying Standard Procedures for Securing Evidence (CIA)

Standard procedures that make it possible to forensically secure volatile and non-volatile data as completely as possible SHOULD be created for applications, IT systems and IT system groups with increased protection needs, as well as for distributed system configurations.

The relevant system-specific standard procedures SHOULD be implemented by proven (and preferably automated) processes. Furthermore, they SHOULD be supported by checklists and technical tools – for example, by software, software tools on mobile storage media and forensic IT hardware such as write-blockers.

DER.2.2.A15 Conducting Drills on Securing Evidence (CIA)

All employees involved in forensic analyses SHOULD regularly practise how to secure evidence in case of an IT security incident.

Additional Information

For more information about threats and security safeguards for module DER.2.2 *Provisions for IT Forensics*, see the following publications, among others:

[BSIFor]	Leitfaden Erstellung von Kryptokonzepten [Guidelines for IT Forensics]: Federal Office for Information Security (BSI), Version 1.0.1, March 2011, https://www.bsi.bund.de/
----------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	DE/Themen/Cyber-Sicherheit/Dienstleistungen/IT-Forensik/forensik_node.html , last accessed on 26.07.2018
[ISFTM24]	The Standard of Good Practice for Information Security : Area TM 2.4 Forensic Investigations, Information Security Forum (ISF), June 2018
[ISO27042]	ISO/IEC 27042:2015: Information technology - Security techniques - Guidelines for the analysis and interpretation of digital evidence, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, June 2015
[ISO27043]	DIN EN ISO/IEC 27043:2015: Information technology - Security techniques - Incident investigation principles and processes, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, March 2015
[NIST80086]	Guide to Integrating Forensic Techniques into Incident Response: NIST Special Publication 800-86, August 2006, https://csrc.nist.gov/publications/detail/sp/800-86/final , last accessed on 26.07.2018
[RFC3227]	Guidelines for Evidence Collection and Archiving: RFC 3227, Internet Engineering Task Force (IETF), February 2002, https://tools.ietf.org/html/rfc3227 , last accessed on 26.07.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module DER.2.2 *Provisions for IT Forensics*:

G 0.17 Loss of Devices, Storage Media and Documents

G 0.20 Information or Products from an Unreliable Source

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.37 Repudiation of Actions

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.17	G 0.20	G 0.22	G 0.25	G 0.27	G 0.29	G 0.31	G 0.37	G 0.45	G 0.46
DER.2.2.A1						X			X	
DER.2.2.A2	X	X	X	X			X		X	X
DER.2.2.A3					X		X		X	
DER.2.2.A4				X					X	X
DER.2.2.A5	X	X	X	X			X		X	X
DER.2.2.A6		X					X		X	X
DER.2.2.A7							X		X	X
DER.2.2.A8	X		X				X	X	X	X
DER.2.2.A9	X		X				X	X	X	X
DER.2.2.A10	X		X				X	X	X	X
DER.2.2.A11	X		X	X			X	X	X	X
DER.2.2.A12	X		X					X	X	X
DER.2.2.A13					X		X		X	
DER.2.2.A14	X		X	X			X	X	X	X
DER.2.2.A15	X		X	X			X	X	X	X



DER.2.3: Clean-Up of Extensive Security Incident

Description

Introduction

Advanced Persistent Threats (APT) are targeted cyber attacks on specific organisations and institutions in which an attacker gains permanent access to a network and then extends this access to other IT systems. These attacks, which are generally difficult to detect, are characterised by a high level of resource deployment and considerable technical capability on the part of the attackers.

After an APT attack has been detected, the persons in charge in the organisations affected face the challenge of having to perform cleaning that exceeds the normal approach to handling IT security incidents. This is because it has to be assumed that the discovered attackers have already been accessing the IT infrastructure affected for a considerable time and used complex attack tools to circumvent the default security mechanisms and establish various backdoors. Furthermore, there is the risk that the attackers are observing the infected environment in detail and will react to cleaning attempts by erasing their traces and sabotaging the investigation.

In general, the module assumes a significant threat landscape involving a focused, motivated attacker with extraordinary resources. As a matter of principle, a (certified) forensics expert should always be consulted in the event of an incident like this if the organisation does not have any corresponding experts of its own. Forensics experts should be consulted as early as the forensic analysis phase, or at least in an advisory role during the cleaning process.

Objective

This module describes what an organisation should do in order to clean its IT systems and restore the normal and secure operating condition of its information domain after an APT attack.

Not in Scope

An information domain may only be cleaned after an APT incident has been detected successfully and analysed forensically. However, detection and forensics are not a subject of this module; they are addressed in DER.1 *Detection of Security-Relevant Events* and DER.2.2 *Provisions for IT forensics*.

In the present module, only the process of cleaning APT incidents is considered. Common incidents are addressed in module DER.2.1 *Security Incident Handling*. The module also does not describe how "indicators of compromise" (IoC, which are traces of a penetration) have to be de-

rived and how these may be used in order to identify recurring attackers. In addition, it does not address how backdoors that may have been overlooked during analysis and cleaning can be found. Moreover, this module is to be distinguished from the overarching incident management process (see DER.2.1 *Security Incident Handling*) in which the process of cleaning is embedded.

Furthermore, attacks in which attackers gain physical access to an IT environment are not considered. As a consequence, attacks that involve breaking into a data centre, bribing administrators, intercepting or manipulating newly procured hardware or eavesdropping on electromagnetic radiation are not covered by this module. Only cyber attacks are considered.

Threat Landscape

For module DER.2.3 *Clean-Up of Extensive Security Incidents*, the following specific threats and vulnerabilities are of particular importance:

Incomplete Cleaning

APT attackers normally aim to infiltrate an information domain permanently. They have access to the necessary resources and are capable of performing long-term attack campaigns. To this end, they use tools and methods that are tailored to a specific target. Even if an APT incident is detected, it cannot be assumed that all access routes of the attackers have been found, all infections and malware communication channels have been eliminated and all backdoors removed. If an incomplete cleaning process is conducted, however, it is very likely that an attacker will regain access to the IT systems and start to broaden his/her access at a later point in time (e.g. after a longer period of inactivity). For example, this can be done both by placing backdoors in operating systems and application software and by manipulating hardware-oriented components (e.g. firmware). Such modifications are very hard to identify, and very few people have the expertise required to extract and analyse them. If the persons in charge try to clean the IT components by overwriting or updating the firmware (for example), the attacker may have also modified the update routines in order to re-enter the system.

Destruction of Traces

After an APT incident, IT systems are often installed from scratch or decommissioned entirely. However, if no forensic copy has been made of the IT systems beforehand, traces may be destroyed that would be required in order to further clarify the incident or even assemble a corresponding court case.

Premature Alarming of the Attacker

Normally, an attack is observed and analysed forensically over a longer period of time before an APT incident is cleaned. Here, the purpose of cleaning is to identify all the access paths, tools and methods in use. If the attacker notices that they have been discovered during this phase, they might take countermeasures. They may, for example, try to cover their tracks or quickly sabotage additional IT systems. They might also stop or create new backdoors in order to continue the attack at a later point in time.

Since it must basically be assumed that the entire IT infrastructure of the organisation has been compromised by an APT attack, the risk is high that the attacker will detect cleaning activities. This is particularly applicable if the compromised IT infrastructure is used in order to plan and coordinate the cleaning process. If essential steps for cleaning are not performed in

the correct order and critical safeguards are not performed simultaneously in a coordinated manner, this will increase the risk of the attacker being alarmed. If the persons in charge isolate the network in a step-by-step manner instead of all at once, for example, the attacker may be warned before their access is terminated effectively.

Data Loss and Failure of IT Systems

When cleaning up an APT incident, different IT systems are installed anew and networks are isolated temporarily. As a consequence, IT systems will inevitably fail and services may only be available to a limited extent or not at all, for example. If the cleaning process takes a very long time, this may result in significant production losses. This in turn may cause significant economic losses that could even threaten the existence of a company. This is particularly the case if insufficient documentation, or none at all, is available for recovery.

Lack of Network Restructuring After an APT Attack

In the event of an APT attack, the attacker obtains detailed knowledge of how the target environment is structured and configured. For example, they become familiar with the existing network segments; naming schemes for IT systems, user and service accounts; and the software and services used. This knowledge may enable the same attacker to regain access to the target environment after a cleaning process. As a consequence, they may move within the network in a targeted, efficient, and unobtrusive manner and achieve a new high degree of infection in no time.

Requirements

The specific requirements of module DER.2.3 *Clean-Up of Extensive Security Incidents* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO), Head of IT

Basic Requirements

For module DER.2.3 *Clean-Up of Extensive Security Incidents*, the following requirements **MUST** be implemented as a matter of priority:

DER.2.3.A1 Creation of a Management Committee [Chief Information Security Officer (CISO)]

In order to clean up an APT incident, a management committee **MUST** be created to plan, coordinate and monitor all necessary activities. The committee **MUST** be provided with all the managerial authority necessary for its tasks.

If a management committee of this kind was already in place when the APT incident was detected and classified, the same committee **SHOULD** also plan and oversee the cleaning process.

If a specialised forensic service provider has already been consulted regarding the analysis of the APT incident, this provider SHOULD also be consulted regarding incident cleaning.

If the IT is too heavily compromised or the necessary cleaning measures are very comprehensive, it SHOULD be checked whether a crisis team should be established. In this case, the management committee MUST monitor the cleaning measures. The management committee MUST report to the crisis team in this case.

DER.2.3.A2 Deciding on a Clean-Up Approach [Chief Information Security Officer (CISO), Head of IT]

Before an APT incident is actually cleaned, the management committee MUST define a cleaning strategy. In so doing, it MUST be decided in particular whether the malware may be removed from compromised IT systems, whether IT systems have to be installed again, or whether IT systems (including the hardware) should be replaced completely. Furthermore, it MUST be defined which IT systems will be cleaned. These decisions MUST be based on the results of a previous forensic examination.

All IT systems affected SHOULD be installed again. Afterwards, the recovery schemes of the organisation MUST be used. However, before backups can be installed, forensic examinations MUST be performed to ensure that no manipulated data or programs are transferred to the newly installed IT system as a consequence.

If an organisation decides that it does not want to reinstall all IT systems, a targeted APT clean-up process MUST be implemented. In order to minimise the risk of backdoors being overlooked, the IT systems MUST be monitored as to whether they still communicate with the attacker in a targeted manner upon completion of the cleaning process.

DER.2.3.A3 Isolation of Affected Network Segments

The network segments affected by an APT incident MUST be isolated (cut off) completely. In particular, the network segments affected MUST NOT be connected to the Internet. In order to effectively lock out the attacker and to prevent them from erasing their traces or sabotaging other IT systems, the network segments MUST be isolated simultaneously.

The network segments to be isolated MUST be determined in advance with the help of a forensic analysis. In so doing, all segments affected MUST be identified. If this cannot be guaranteed, all suspicious network segments MUST be isolated along with all those that are only theoretically infected.

In order to effectively isolate network segments, all local Internet connections (e.g. additional DSL connections in individual subnets) MUST be captured and taken into consideration as completely as possible.

DER.2.3.A4 Blocking and Changing Access Data and Cryptographic Keys

Since it must be assumed that the attacker has obtained all the access data present on the compromised IT systems, all access data MUST be changed after the network is isolated. Furthermore, access data managed in a centralised manner MUST also be reset, including in Active Directory environments or when the Lightweight Directory Access Protocol (LDAP) has been used.

If the central authentication server (domain controller or LDAP server) has been compromised, all the users on it MUST be blocked and their passwords MUST be changed. This MUST be im-

plemented by experienced administrators – if necessary, with the help of internal or external forensics experts.

If TLS keys or an internal certification authority (CA) has been compromised by the APT attack, corresponding keys and infrastructures **MUST** be created and distributed anew. The compromised keys **MUST** be blocked reliably, as well.

DER.2.3.A5 Closing the Initial Entry Route

If a forensic examination determines that the attacker used a technical vulnerability to penetrate the network of the organisation, this vulnerability **MUST** be closed. If the attackers were able to compromise the IT systems as a consequence of human error, organisational, personnel, and technical measures **MUST** be taken in order to prevent similar incidents in the future.

DER.2.3.A6 Returning to Production Operations

After the network has been cleaned successfully, the IT systems **MUST** be returned to production operations in a controlled manner. In so doing, all IT systems previously procured and programs previously installed that were used to observe and analyse the attack **MUST** either be removed or put into production operation. The same **MUST** be done with communication and collaboration systems procured for the purpose of cleaning. Evidence and decommissioned IT systems **MUST** either be deleted or destroyed securely, or archived appropriately.

Standard Requirements

For module DER.2.3 *Clean-Up of Extensive Security Incidents*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

DER.2.3.A7 Targeted System Hardening

After an APT attack, all IT systems affected **SHOULD** be hardened. This **SHOULD** be based on the results of the forensic examinations (see DER.2.X *Forensic IT Analyses*). In addition, it **SHOULD** be checked again whether the environment affected is still secure (e.g. using the results of the comprehensive forensic analyses).

If possible, IT systems **SHOULD** already be hardened as they are being cleaned. Safeguards that cannot be performed on short notice **SHOULD** be added to an action plan and implemented in the medium term. The CISO **SHOULD** be responsible for drawing up the plan and checking whether the plan was implemented properly.

DER.2.3.A8 Establishing Secure, Independent Communication Channels

Secure communication channels **SHOULD** be established for the management committee and the employees charged with cleaning. It **SHOULD** be ensured that the communication channel selected is as secure as possible.

Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.2.3 *Clean-Up of Extensive Security Incidents* are listed below for requirements which go beyond the standard level of protection. These **SHOULD** be taken into account **IN THE EVENT OF INCREASED PROTECTION NEEDS**. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

DER.2.3.A9 Hardware Replacement in Affected IT Systems (CIA)

In cases involving IT systems with high protection needs, it SHOULD be considered whether the hardware needs to be replaced completely after an APT incident. If suspicious behaviour (e.g. inexplicable network traffic) is still being observed even after cleaning the individual IT systems, the IT system affected SHOULD be replaced.

DER.2.3.A10 Conversions for Making Another Attack by the Same Attacker More Difficult (CI)

In order to prevent the same attacker from performing another APT attack on the IT systems of the organisation, the internal design of the network environment SHOULD be changed. Furthermore, mechanisms SHOULD be established that can be used to quickly detect a recurring attacker.

Additional Information

For more information about threats and security safeguards for module DER.2.3 *Clean-Up of Extensive Security Incidents*, see the following publications, among others:

[CS072]	Erste Hilfe bei einem APT Angriff [First Aid in the Event of an APT Attack]: BSI publications on cyber security (BSI-CS 072), Version 3.0, January 2016, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_072_TLP-White.pdf , last accessed on 05.10.2018
[DRP]	Data Breach Response Guide: Experian Data Breach Resolution, 2013 https://www.experian.com/assets/data-breach/brochures/response-guide.pdf , last accessed on 05.10.2018
[KGT]	CERT-EU Security White Paper, Protection from Kerberos Golden Ticket: Mitigating pass the ticket on Active Directory, CERT-EU, July 2014, https://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf , last accessed on 05.10.2018
[ReCoBS]	Common Criteria Protection Profile for Remote-Controlled Browsers System (Re-CoBS):BSI-PP-0040, Federal Office for Information Security (BSI), Version 1.0, February 2008, https://www.commoncriteriaportal.org/files/ppfiles/pp0040b.pdf , last accessed on 11.09.2018
[SANS1]	White Paper, When Breaches Happen: Top Five Questions to Prepare For: SANS Institute, June 2012, https://www.sans.org/reading-room/whitepapers/analyst/breaches-happen-top-questions-prepare-35220 , last accessed on 05.10.2018
[SANS2]	Detection and Recovery from a Major security Breach: Richard Hanschu, SANS Institute, 2000, https://giac.org/paper/gcux/50/detection-recovery-major-security-breach/100810 , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module DER.2.3 *Clean-Up of Extensive Security Incidents*:

- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.19 Disclosure of Sensitive Information
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.24 Destruction of Devices or Storage Media
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.39 Malware
- G 0.40 Denial of Service
- G 0.41 Sabotage
- G 0.42 Social Engineering
- G 0.43 Attack with Specially Crafted Messages
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0.1 4	G 0.1 5	G 0.1 6	G 0.1 9	G 0.1 8	G 0.2 0	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 4	G 0.2 8	G 0.2 9	G 0.3 1	G 0.3 2	G 0.3 9	G 0.4 0	G 0.4 1	G 0.4 2	G 0.4 3	G 0.4 5	G 0.4 6
DER.2.3.A1	X			X												X	X	X		X	X
DER.2.3.A2	X	X	X	X			X	X	X	X				X	X		X		X	X	X
DER.2.3.A3	X			X				X	X					X						X	X
DER.2.3.A4	X	X	X	X			X	X	X	X				X	X	X	X		X	X	X
DER.2.3.A5	X	X		X					X		X			X			X	X			
DER.2.3.A6				X	X						X	X	X								
DER.2.3.A7	X	X	X	X		X	X	X	X	X	X			X	X	X	X		X	X	X
DER.2.3.A8	X	X	X	X				X											X	X	X
DER.2.3.A9	X	X	X	X			X	X	X						X		X		X		X
DER.2.3.A10	X	X	X	X			X	X	X	X	X			X	X		X		X		X



DER.3.1: Audits and Revisions

Description

Introduction

Audits and revisions are fundamental for every successful information security management system (ISMS). Auditing established security safeguards and processes at regular intervals as to whether they are effective, complete, appropriate and still up to date is the only way to assess the overall state of information security. Hence, audits and revisions are a tool to be used to determine, achieve and maintain an appropriate level of security. Using this tool, it is possible to identify improper developments and existing security shortcomings and to initiate corresponding countermeasures.

The term audit (from the Latin *audire* = hear, listen) refers to a systematic, independent examination of activities and corresponding results regarding their compliance with defined requirements (e.g. standards or guidelines). Within the framework of a revision (revise = control, check), it is checked whether documents, conditions, objects or methodologies are correct, effective and appropriate. As opposed to an audit, a revision does not necessarily have to be performed independently. Moreover, a revision may already include remedial actions for the purpose of maintenance.

Objective

This module defines requirements for audits and revisions in order to improve information security in an organisation, avoid improper developments in this area and optimise security safeguards and processes.

Not in Scope

This module describes how audits and revisions can be planned, implemented and revised from the perspective of an ISMS. As a result, it covers internal audits ("first-party" audits) and revisions, as well as audits with service providers and partners ("second-party" audits) of the organisation. Certification audits ("third-party" audits) are not taken into consideration in this module.

The IS audits that are obligatory for federal government agencies is not considered either. These are covered in module DER 3.2 *Audits Based on the BSI "Guideline for IS Audits"*. Moreover, the question of how audits and revisions may be integrated into an overarching auditing body that may exist within an organisation is not taken into consideration.

Threat Landscape

The following specific threats and vulnerabilities are of particular importance for module DER.3.1 *Audits and Revisions*:

Insufficient or Unplanned Implementation of Security Safeguards

The level of protection of an organisation depends on security safeguards being implemented completely and correctly. In particular during the critical phases of projects or under certain framework conditions, security safeguards may be suspended temporarily. The need to reactivate them is sometimes forgotten, however, which results in an insufficient level of security.

Ineffective or Inefficient Implementation of Security Safeguards

If security safeguards are implemented without considering certain practical aspects, the safeguards might be ineffective. For example, it does not make any sense to block the entrance area using turnstiles if employees can easily access the building using an open side entrance.

Individual safeguards may also be implemented that do not make any sense from an economic point of view. Hence, a properly implemented rights and role concept is more reasonable and economic for protecting information with normal levels of confidentiality than establishing a certificate authority and subsequent certificate-based encryption of the file server.

Insufficient Implementation of the ISMS

In many organisations, the Chief Information Security Officer checks whether the security safeguards have been implemented. The auditing of the ISMS itself is often forgotten, in particular because this should be done by an independent third party. As a consequence, the processes of an ISMS might be implemented inefficiently or inappropriately. The level of security of the organisation may thus be impaired.

Insufficient Qualification of the Auditor

If an auditor or revisor is qualified insufficiently or insufficiently prepared, they might incorrectly assess the security status of an organisation during the audit or revision. As a consequence, they may not prescribe the necessary corrective measures (or even call for improper measures) in their audit report. In the worst case, this leads to excessive (and thus non-economic) protection of information, or insufficient protection that entails a great many risks.

Lack of Long-Term Planning

If audits and revisions are not planned in a long-term, centralised manner, individual areas may be audited very frequently, and others not at all. As a consequence, it may be very difficult or not possible at all to assess the security status of the information domain.

Lack of Planning and Coordination When Performing an Audit

If an audit is planned insufficiently and not coordinated with all involved employees of the organisation, the required contact persons may not be available during the on-site audit. As a result, it may be impossible to audit individual areas at all. If the auditor has set too tight a schedule for the individual areas, the audit might only be performed superficially due to a lack of sufficient time.

Lack of Coordination with Employee Representatives

Audits and revisions may also examine aspects that can be used to draw conclusions on the performance of employees. Hence, these audits and revisions may be considered a performance evaluation. If the Employee Representatives are not involved, this may result in violations of the applicable right of co-determination.

Deliberate Concealment of Deviations

Employees might be afraid of errors being discovered within the framework of the audit and, as a consequence, try to conceal security issues. This might convey an incorrect picture of the actual status quo.

Requirements

The specific requirements of module DER.3.1 *Audits and Revisions* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for compliance with the requirements. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Top Management, Audit Team Leader, Audit Team

Basic Requirements

For module DER.3.1 *Audits and Revisions*, the following requirements **MUST** be implemented as a matter of priority.

DER.3.1.A1 Definition of Responsibilities [Top Management]

The organisation's top management **MUST** appoint an employee who will be responsible for planning and initiating audits and revisions. In so doing, it **MUST** be observed that no conflicts of interest are caused (e.g. if one's own department is to be audited). The person responsible **MUST** monitor the processing of the results of the audits and revisions.

DER.3.1.A2 Preparation of an Audit or Revision

Prior to an audit or revision, the object and objectives **MUST** be defined. The contact persons affected **MUST** be informed, as well. Depending on the object of the audit or revision, the Employee Representatives **MUST** also be informed of the planned audit or revision.

DER.3.1.A3 Performing an Audit

Within the framework of an audit, compliance with the requirements of directives, standards and so on **MUST** be checked. The audited organisation **MUST** be familiar with the requirements.

An audit **MUST** include a document revision and an on-site audit. Within the framework of the on-site audit, it **MUST** be ensured that the auditors never actively interfere with IT systems and do not issue any instructions regarding changes to the object of the audit either.

All results of an audit **MUST** be documented in writing and summarised in an audit report. The audit report **MUST** be submitted to the contact person of the organisation in a timely manner.

DER.3.1.A4 Performing a Revision

Within the framework of a revision, it **MUST** be checked whether the requirements are complete, correct, appropriate and currently implemented. Deviations identified **MUST** be corrected immediately whenever possible. The respective revisions **MUST** be documented using a revision history.

Standard Requirements

For module DER.3.1 *Audits and Revisions*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

DER.3.1.A5 Integration into the Information Security Process

A policy on internal ISMS auditing and a policy on controlling corrective measures **SHOULD** be drawn up. The policies **SHOULD** specify that regular audits and revisions are part of the security process and are initiated by the security process.

Furthermore, it **SHOULD** be ensured that the results of the audits and revisions are returned to the ISMS and incorporated into its improvement. Moreover, the audits and revisions performed, the results and the activities undertaken to remedy shortcomings and improve quality **SHOULD** be incorporated into the regular report of the Chief Information Security Officer to the organisation's top management.

DER.3.1.A6 Definition of the Audit and Revision Basis and a Uniform Evaluation Scheme

A uniform audit basis **SHOULD** be defined. A uniform evaluation scheme **SHOULD** be defined and documented for evaluating the implementation of requirements.

DER.3.1.A7 Drawing Up an Audit Program

An audit program **SHOULD** be drawn up that contains all audits and revisions to be performed in the next several years. Objectives **SHOULD** be defined for the audit program that are derived in particular from the organisation's objectives and the information security objectives.

Reserves **SHOULD** be set aside in the annual resource plan for unforeseeable events. The audit program **SHOULD** be subject to its own continuous improvement process.

DER.3.1.A8 Creation of a Revision List

One or more revision lists **SHOULD** be maintained that document the current status of the revision objects and the scheduled revisions.

DER.3.1.A9 Selection of an Appropriate Audit or Revision Team

For every audit and revision, a suitable team **SHOULD** be assembled. A senior auditor (Audit Team Leader) or revisor **SHOULD** be appointed who will be responsible for the overall performance of the audits and revisions.

The size of the audit and revision team **SHOULD** be in accordance with the area to be audited. In this regard, the competence requirements of the audit subjects and the size and the local

distribution of the area to be audited SHOULD be taken into consideration in particular. The members of the audit and revision team SHOULD be appropriately qualified.

The neutrality of the audit team SHOULD be guaranteed. The revisors SHOULD be independent, as well. If external service providers are deployed as auditors or revisors, they SHOULD be checked regarding their independence and obliged to maintain confidentiality.

DER.3.1.A10 Creation of an Audit or Revision Plan [Audit Team Leader]

Prior to an audit or a major revision, the Audit Team Leader or the lead revisor SHOULD create an audit or revision plan. For audits, the Gap Analysis Plan SHOULD be part of the final audit report. The Gap Analysis Plan SHOULD be updated during the entire audit and be adjusted as required. Minor revisions SHOULD be scheduled according to the revision list.

Sufficient resources SHOULD be provided for the audit or revision team.

DER.3.1.A11 Communication and Behaviour During Audits [Audit Team Leader]

There SHOULD be clear rules as to how the audit or revision team and the employees of the organisation or department to be audited may exchange information with one another. This way, suitable safeguards SHOULD be implemented to ensure that the information exchanged within the framework of an audit remains confidential and its integrity remains intact.

Persons supporting the audit SHOULD NOT influence the audits. Furthermore, they SHOULD be obliged to maintain confidentiality.

DER.3.1.A12 Holding an Initial Meeting [Audit Team Leader]

An initial meeting between the audit or revision team and the contact persons concerned SHOULD be held. In so doing, the audit or revision method SHOULD be explained and the framework conditions of the on-site audit SHOULD be coordinated and confirmed by the person responsible in each case.

DER.3.1.A13 Inspection and Review of Documents [Audit Team]

Within the framework of audits, documents SHOULD be reviewed based on the requirements specified in the Gap Analysis Plan. All relevant documents SHOULD be reviewed as to whether they are up to date, complete and comprehensible. The results of the document review SHOULD be documented. The results SHOULD be incorporated into the on-site audit whenever it makes sense.

DER.3.1.A14 Selection of Samples [Audit Team]

The audit team SHOULD select the samples for the on-site audit in a risk-oriented manner and justify and document them in a comprehensible way. If the audit is performed on the basis of module target objects and safeguards, these SHOULD be selected on the basis of a previously defined method. When selecting samples, the results of previous audits SHOULD be taken into consideration, as well.

DER.3.1.A15 Selection of Appropriate Audit Techniques [Audit Team]

The audit team SHOULD use techniques appropriate for the subject matter to be audited in each case – for example, interviews (see DER.3.1.A18 *Conducting Interviews*) or document audits. Furthermore, it SHOULD be ensured that all audits are proportionate to the situation at hand.

DER.3.1.A16 Schedule of the On-Site Audit [Audit Team]

Together with the contact persons, the audit team SHOULD draw up the schedule for the on-site audit. The results SHOULD be documented in the Gap Analysis Plan.

DER.3.1.A17 Performance of the On-Site Audit [Audit Team]

At the beginning of the on-site audit, the audit team SHOULD hold an initial meeting with the persons in charge at the organisation concerned. Afterwards, all requirements specified in the Gap Analysis Plan SHOULD be audited using the audit techniques defined. If a selected sample deviates from the documented status, the sample SHOULD be extended as needed until the issue is clarified. After the audit, the audit team SHOULD hold a closing meeting in which the results (without any evaluation) and next steps are briefly presented. The meeting SHOULD be documented in writing.

DER.3.1.A18 Conducting Interviews [Audit Team]

Interviews SHOULD be conducted in a structured manner. Questions SHOULD be concise, precise and easily understandable. In addition, appropriate interviewing techniques SHOULD be used.

DER.3.1.A19 Revision of the Risk Treatment Plan [Audit Team]

The audit team SHOULD check whether the remaining residual risks are appropriate and sustainable for the information domain. It SHOULD also check whether they are supported by the top management in a binding manner. Safeguards that fundamentally contribute to the information security of the entire organisation MUST NOT be incorporated into the risks assumed.

The auditor SHOULD verify at random whether and to what extent the safeguards defined in the risk treatment plan have been implemented.

DER.3.1.A20 Final Meeting [Audit Team]

The audit team SHOULD conduct a closing meeting with the respective persons in charge at the audited organisation. Within the framework of this meeting, the preliminary audit results and the next steps SHOULD be presented.

DER.3.1.A21 Analysis of Audits [Audit Team]

After the on-site audit, the information collected SHOULD be consolidated further and analysed. After any additional information and additional documentation required after the fact are analysed, the safeguards audited SHOULD be subjected to a final evaluation. A sufficient time period SHOULD be granted for the provision of documentation requested after the fact. Documents not received by the agreed final date SHOULD be considered non-existent.

DER.3.1.A22 Creation of an Audit Report [Audit Team]

The audit team SHOULD transfer the results obtained into an audit report and document them transparently therein. The results of the audit SHOULD be explained to the persons in charge in a presentation.

The organisation audited SHOULD ensure that all entities affected are provided with the parts of the audit report that are important and necessary for them within an appropriate period.

DER.3.1.A23 Documentation of Revision Results

The results of a revision SHOULD be uniformly documented.

DER.3.1.A24 Conclusion of the Audit or Revision [Audit Team]

After the audit or revision, all relevant documents, storage media and IT systems SHOULD be returned or destroyed. This SHOULD be coordinated with the organisation audited. In doing so, storage obligations resulting from legal or other binding requirements SHOULD be taken into account accordingly. Furthermore, the CISO SHOULD have all the forms of access granted to the audit or revision team disabled or deleted.

There SHOULD be an agreement with the auditors or revisors as to how the results are to be handled. Here, it SHOULD also be established that the audit results must not be forwarded to other organisations without the consent of the organisation audited.

DER.3.1.A25 Wrap-Up and Initiation of the Follow-Up Phase

The deviations or shortcomings identified in the audit report or within the framework of a revision SHOULD be remedied within a reasonable period of time. In order to ensure that the implementation status can be comprehended easily, the corrective measures to be performed, including the respective times and responsibilities, SHOULD be documented. Corrective measures that have already been completed SHOULD also be documented. There SHOULD already be an established procedure in the ISMS that is to be used for this purpose.

In the event of serious deviations or shortcomings, the audit or revision team SHOULD check whether the corrective measures have been performed.

DER.3.1.A26 Monitoring and Adapting the Audit Program

The audit program SHOULD be monitored and adapted continuously to ensure compliance with regard to dates, audit objectives, audit contents and audit quality.

With the help of the existing requirements for the audit program and the results of the audits performed, it SHOULD be checked whether the audit program is appropriate. It should be adapted as required.

DER.3.1.A27 Storage and Archiving of Documents on Audits and Revisions

Audit programs and documents on audits and revisions SHOULD be stored and kept in accordance with the applicable laws and any other regulatory requirements in a transparent and audit-compliant manner. In so doing, it SHOULD be ensured that only authorised persons may access audit programs and documents (particularly audit reports). Upon expiration of the archiving periods, the audit programs and documents SHOULD be destroyed securely.

Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.3.1 *Audits and Revisions* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

DER.3.1.A28 Security Checks on Auditors (CI)

If auditors must access particularly sensitive information, certificates regarding their integrity and reputation SHOULD be requested. If the material is classified as confidential information, the members of the audit team SHOULD be subjected to a security check in accordance with the German Security Screening Act (SÜG). In this regard, the CISO SHOULD involve the Confidentiality Officer or Security Representative of the organisation.

Additional Information

For more information about threats and security safeguards for module DER.3.1 *Audits and Revisions*, see the following publications, among others:

[19011]	ISO 19011:2011: Guidelines for auditing management systems, International Organization for Standardization (ed.), ISO/TC 176/SC 3, November 2011
[27007]	ISO/IEC 27007:2011: Information technology - Security techniques - Guidelines for information security management systems auditing, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2017
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module DER.3.1 *Audits and Revisions*:

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.18	G 0.19	G 0.27	G 0.29	G 0.46
DER.3.1.A1	X		X		X
DER.3.1.A2	X			X	
DER.3.1.A3	X				
DER.3.1.A4	X				
DER.3.1.A5	X	X			X
DER.3.1.A6	X				
DER.3.1.A7	X			X	X
DER.3.1.A8	X			X	X
DER.3.1.A9	X		X		X
DER.3.1.A10	X				
DER.3.1.A11	X	X			
DER.3.1.A12	X	X			
DER.3.1.A13	X				
DER.3.1.A14	X			X	
DER.3.1.A15	X				
DER.3.1.A16	X				
DER.3.1.A17	X	X			
DER.3.1.A18	X	X			
DER.3.1.A19	X			X	
DER.3.1.A20	X				
DER.3.1.A21	X				

DER.3.1.A22	X			X	X
DER.3.1.A23	X			X	X
DER.3.1.A24	X	X		X	X
DER.3.1.A25	X			X	
DER.3.1.A26	X		X	X	X
DER.3.1.A27	X				X
DER.3.1.A28	X		X	X	X



DER.3.2: Audits Based on the BSI “Guideline for IS Audits”

Description

Introduction

An information security audit (IS audit) based on IT-Grundschutz is a particular type of audit based on the “Guideline for IS Audits”. An IS audit based on IT-Grundschutz is a random check of an information security management system (ISMS). It is characterised by an holistic approach. This means that all levels of an ISMS are checked, from the establishment of an information security organisation and personnel aspects to the configuration of IT systems and applications. Economic efficiency and compliance, which are the focus of traditional IT audits, are only of secondary importance. Information security (including the adequacy of the security measures) is thus the essential test criterion of an IS audit based on IT-Grundschutz.

An IS audit based on IT-Grundschutz is always a fundamental part of successful information security management. Only by regularly checking the established measures and information security processes is it possible to evaluate whether they are effectively implemented, complete, up-to-date and appropriate. An IS audit based on IT-Grundschutz is therefore a suitable tool for determining, achieving, maintaining and continuously improving an appropriate level of security in an organisation.

The main task of the IS audit based on IT-Grundschutz is to support and accompany the top management of the organisation, the IS management team and, in particular, the Chief Information Security Officer (CISO) in achieving the highest possible level of information security in their organisation.

Objective

This module defines requirements for an IS audit based on IT-Grundschutz in order to improve the information security in an organisation, avoid improper developments in this area and optimise security safeguards and processes.

Not in Scope

The ways in which an IS audit based on IT-Grundschutz can be integrated into an existing overarching audit organisation (e.g. an internal auditing department) within an institution are not covered. The module DER.3.2 *Audits Based on the BSI “Guideline for IS Audits”* is a specific example of the requirements described in general in module DER.3.1 *Audits and Revisions*. Organisations that implement this module no longer need to implement DER.3.1 *Audits and Revisions*, as its requirements are fully contained in this module.

For federal agencies, however, the use of module DER.3.2 is mandatory within the framework of IS audits because special requirements from the "Implementation Plan for Ensuring IT Security in the Federal Administration" (UP Bund 2017) apply to these agencies.

IS audits and certification in line with ISO 27001 on the basis of IT-Grundschutz complement each other. IS audits can accompany the path to certification and, in contrast, can be carried out during the initiation of the security process in the organisation. They show the organisation where there is an urgent need for action and which security deficiencies should be addressed as a matter of priority. If individual information domains in the organisation are certified according to ISO 27001 on the basis of IT-Grundschutz, re-certification and IS audits for these information domains should be carried out together if possible. The findings of surveillance audits or certification procedures can be used for IS audits.

If an ISO 27001 certificate based on IT-Grundschutz is available for the entire organisation, the surveillance audits required in the certification procedure replace the IS audits.

Note: The regulations regarding protection and handling of classified information (VSA) remain unaffected and apply regardless of the requirements of this module.

Threat Landscape

For module DER.3.2 *Audits Based on the BSI "Guideline for IS Audits"*, the following specific threats and vulnerabilities are of particular importance:

Violation of Specifications of UP Bund

The 2017 Implementation Plan for the Federal Administration (UP Bund 2017) is the defined guideline for information security in the Federal Administration. It establishes a form of cross-departmental information security management for federal agencies in which each agency is responsible for creating and implementing its specific security concept. In addition to the federal agencies, other organisations may be obliged by law, contract or other regulations to comply with the UP Bund 2017. The UP Bund 2017 explicitly stipulates that the BSI standards on information security and IT-Grundschutz, as well as the procedure for standard protection described therein, must be implemented as a minimum requirement. Furthermore, the UP Bund 2017 stipulates that all organisations that are obliged to implement the plan must regularly review the status of their own ISMS (e.g. by means of a suitable IS audit) and apply the "*Guideline for Information Security Audits Based on IT-Grundschutz*". If this does not happen, organisations that are obliged to implement the UP Bund 2017 will be in violation of these requirements.

Suspension of Security Safeguards

The level of security within an organisation depends on the complete and correct implementation of security safeguards. Particularly during the critical phases of projects or under certain conditions, security safeguards may be temporarily suspended. In some cases, however, the need to reactivate them may be forgotten, resulting in an insufficient security level.

Ineffective or Inefficient Implementation of Security Safeguards

If security safeguards are implemented without considering the practical aspects at hand, the safeguards might be ineffective. For example, it does not make any sense to block the entrance area using turnstiles if employees can easily access the building using an open side entrance.

Individual safeguards may also be implemented that do not make any sense from an economic point of view. To protect information with normal protection needs with regard to confidentiality, an appropriately implemented rights and role concept makes more sense and is more economical than establishing a certificate authority and encrypting all information on the file server using certificates.

Inadequate Implementation of the Information Security Management System

In many organisations, the Chief Information Security Officer (CISO) checks whether the security safeguards have been implemented. The examination of the actual ISMS can often be forgotten because the CISO is part of the ISMS, and thus not impartial. As a result, the processes of an ISMS may have been inefficiently or inadequately implemented and the organisation's security level may be unintentionally low.

Insufficient Qualification of the Auditor

If IS auditors are not sufficiently qualified or do not sufficiently prepare for audits, they may misjudge the security status of an organisation during an IS audit. As a result, they may not recommend the necessary corrective measures – or even recommend incorrect measures – in their audit report. This can lead to information being protected in an uneconomic or high-risk manner.

Impartiality of Internal IS Audit Teams

Internal employees can be formed into IS audit teams within organisations. If these teams are not sufficiently kept separate from other processes, the IS auditors may be dependent or biased. This is particularly the case if members of the IS audit team are or have been involved in the planning or implementation of the ISMS.

Lack of Long-Term Planning

If IS audits are not planned in a centralised, long-term manner, individual units within an organisation may be audited very frequently, and others not at all. Changes to the ISMS may not be checked sufficiently if audits are only carried out irregularly. In such cases, it is very difficult or even impossible to assess the security status of the information domain.

Insufficient Planning and Coordination When Performing IS Audits

If an IS audit based on IT-Grundschutz is insufficiently planned and not coordinated with all the employees involved within the organisation, the required contact persons may not be available during the on-site audit. As a result, it may be impossible to audit individual areas at all. If the IS auditors set too tight a schedule for the individual areas and do not factor in enough time, the audit of the organisation may only be superficial.

Lack of Coordination with Employee Representatives

IS audits based on IT-Grundschutz can also cover aspects that enable conclusions to be drawn on employee conduct and performance. These audits may therefore be considered as conduct and performance appraisals. If the Employee Representatives are not involved, the on-site audit may be delayed or even cancelled.

Deliberate Concealment of Deviations or Problems

Employees may fear that their own errors will be discovered during an IS audit. To avoid this, they could conceal security problems and thus give a false impression of the actual level of security. This allows security deficiencies to remain undiscovered and uncorrected. In addition, the risk associated with this lack of security remains unknown to and unassessed by the top management.

Loss of Confidentiality of Sensitive Information

During an IS audit based on IT-Grundschutz, the IS auditors collect confidential information (such as on vulnerabilities and attack options). They may also identify shortcomings in the information security of the audited organisation. However, if these shortcomings become known to unauthorised third parties, they could be used to attack or defame the organisation.

Requirements

The specific requirements of module DER.3.2 *Audits Based on the BSI "Guideline for IS Audits"* are listed below. As a matter of principle, the person responsible for the IS audit is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Person in Charge of IS Audit
Further Roles	Chief Information Security Officer (CISO), Top Management, IS Audit Team

Basic Requirements

For module DER.3.2 *Audits Based on the BSI "Guideline for IS Audits"*, the following requirements **MUST** be implemented as a matter of priority:

DER.3.2.A1 Designation of Persons in Charge of the IS Audit

The organisation **MUST** designate a person in charge of IS auditing. This person **MUST** plan and initiate IS audits and track their results.

DER.3.2.A2 Creation of an IS Audit Manual

An IS audit manual **MUST** be prepared that contains the objectives to be achieved, legal requirements to be met, information about the organisation and the resources and the framework conditions. It **MUST** also describe how to archive the documentation. The manual **MUST** be approved by the top management level.

DER.3.2.A3 Definition of the Audit Basis [IS Audit Team]

The BSI Standards 200-1 to 200-3 and the IT-Grundschutz Compendium **MUST** be the basis for the IS audit. Standard IT-Grundschutz protection **SHOULD** be used for this. These audit principles **MUST** be known to all parties involved.

DER.3.2.A4 Drawing Up a Plan for the IS Audit

Organisations that are not entirely ISO 27001-certified on the basis of IT-Grundschutz **MUST** have an IS partial audit or an IS cross-cutting audit carried out at least every three years. In addition, further audits should be planned if the information domain is significantly changed.

The person in charge of the IS audit should draw up a rough multi-year plan for audits. This schedule **SHOULD** then be made more specific in a detailed one-year schedule.

DER.3.2.A5 Selection of an Appropriate IS Audit Team

A team consisting of at least two IS auditors **MUST** be assembled or commissioned. The IS audit team **MUST** be granted unlimited information and inspection rights for its activities. In internal IS audit teams, the individual IS auditors **MUST** be impartial. The members of an IS audit team **MUST NOT** be or have been involved in planning or implementing the ISMS.

DER.3.2.A6 Preparation of an IS Audit [Top Management]

Top management **MUST** initiate the IS audit procedure. They **MUST** commission the IS audit team to carry out an IS audit. The IS audit team **MUST** determine the reference documents required for an IS audit. The organisation to be audited **MUST** hand over the security concept and all other necessary documents to the IS audit team.

DER.3.2.A7 Performance of an IS Audit [IS Audit Team]

Within the framework of an IS audit, a document audit and an on-site audit **MUST** be performed. All results of the two audits **MUST** be documented in writing and summarised in an IS audit report.

Before an IS cross-cutting audit is performed for the first time, an IS partial audit **MUST** be selected as the IS audit procedure. The IS partial audit **MUST** be completed with a positive result before an IS cross-cutting audit is performed.

DER.3.2.A8 Storage of IS Audit Reports

The IS audit report and the reference documents this report is based on **MUST** be stored by the organisation audited in an audit-compliant manner for at least 10 years after the delivery of the report unless different laws or regulations apply. In so doing, it **MUST** be ensured that only authorised persons may access the IS audit reports and the reference documents.

Standard Requirements

For module DER.3.2 *Audits Based on the BSI "Guideline for IS Audits"*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

DER.3.2.A9 Integration into the Information Security Process [Chief Information Security Officer (CISO)]

It **SHOULD** be ensured that IS audits based on IT-Grundschutz are part of and initiated by the security process. Furthermore, the results of IS audits **SHOULD** be returned to the ISMS and incorporated into its improvement.

In addition, the results of the IS audits and the activities to remedy deficiencies and improve quality **SHOULD** be included in the CISO's regular report to the organisation's top management.

DER.3.2.A10 Communication Coordination

There SHOULD be clear rules as to how information is to be exchanged between the IS audit team and the organisation to be audited. This SHOULD ensure that the information exchanged within the framework of an IS audit remains confidential and its integrity remains intact.

DER.3.2.A11 Performance of an Initial Meeting for a Cross-Cutting Audit [IS Audit Team]

When a cross-cutting audit is to be conducted, an initial meeting SHOULD take place between the IS audit team and the contact persons within the organisation to be audited. The meeting SHOULD address the following items:

- presentation and explanation of the IS audit process
- presentation of the organisation (focus of work and overview of the IT used)
- handover of the reference documents to the IS audit team

DER.3.2.A12 Creation of a Gap Analysis Plan [IS Audit Team]

Prior to the IS audit, the IS audit team SHOULD create an IS Gap Analysis Plan. If it is necessary during the audit to extend or otherwise adapt the planned procedures, the IS Gap Analysis Plan SHOULD be adapted accordingly. The Gap Analysis Plan SHOULD also be included in the final IS audit report.

For the IS partial audit, the binding BSI audit subject list SHOULD be used as the Gap Analysis Plan.

DER.3.2.A13 Inspection and Review of Documents [IS Audit Team]

The document revision SHOULD check the requirements defined in the Gap Analysis Plan. The IS audit team SHOULD check whether all relevant documents are up to date and complete. When checking that documents are up to date, the granularity of the documents SHOULD be taken into consideration. Care SHOULD be taken to ensure that all relevant aspects are included and appropriate roles assigned.

Furthermore, it SHOULD be checked whether the present documents and the decisions made therein are transparent. The results of the document revision SHOULD be documented and, when doing so makes sense, incorporated into the on-site audit.

DER.3.2.A14 Selection of Target Objects and Requirements to Be Audited [IS Audit Team]

Within the framework of an IS cross-sectional audit or an IS partial audit, the IS audit team SHOULD select the module target objects for the on-site audit based on the results of the document revision. However, the information security management module (see ISMS.1 *Security Management*) of the IT-Grundschutz Compendium, including all related requirements, SHOULD always be checked completely. A further 30 per cent of the remaining module target objects SHOULD be selected for testing in a risk-based approach. The selection SHOULD be clearly documented. For the module target objects selected in this way, 30 per cent of the respective requirements SHOULD be checked during the IS audit.

In addition, the requirements criticised in previous IS audits SHOULD be taken into account when selecting the module target objects to be tested. All requirements with serious security shortcomings from previous IS audits SHOULD be audited.

DER.3.2.A15 Selection of Appropriate Audit Techniques [IS Audit Team]

It SHOULD be ensured that appropriate audit techniques are used in order to determine the areas to be audited. All audits SHOULD be proportionate.

DER.3.2.A16 Creating a Procedure for the On-Site Audit [IS Audit Team]

Together with the contact person of the organisation to be audited, the IS audit team SHOULD draw up a schedule for the on-site audit. The results SHOULD be documented along with the IS Gap Analysis Plan.

DER.3.2.A17 Performance of the On-Site Audit [IS Audit Team]

The on-site audit SHOULD investigate and determine whether the selected measures meet the requirements of IT-Grundschutz in a practical and adequate manner.

The audit SHOULD start with an initial meeting. All the requirements of the Gap Analysis Plan that are selected for the audit and/or all the subject areas from the audit subject list SHOULD then be checked. The envisaged audit techniques SHOULD be used for this. If deviations from the documented status for a selected sample are identified, the sample SHOULD be extended as required until the matter is clarified.

During the on-site audit, the IS auditors SHOULD never actively interfere with IT systems and SHOULD not issue any instructions regarding changes to the object of the audit either.

All essential issues and information on source, information and presentation requests, as well as meetings held, SHOULD be documented in writing.

In a closing meeting, the IS audit team SHOULD briefly present the main findings to the contact persons of the audited organisation. The IS audit team SHOULD NOT specifically evaluate the findings, but provide indications of possible deficiencies and the further steps to take. Minutes SHOULD also be taken for this closing meeting.

DER.3.2.A18 Conducting Interviews [IS Audit Team]

Interviews SHOULD be conducted in a structured manner. Questions SHOULD be concise, precise and easily understandable. In addition, appropriate interviewing techniques SHOULD be used.

DER.3.2.A19 Reviewing Risk Treatment Options [IS Audit Team]

The IS audit team SHOULD check whether the remaining residual risks are appropriate and sustainable for the information domain and whether the top management accepts responsibility for them in a binding manner. The IS audit team SHOULD randomly verify whether and to what extent the options selected to treat risk have been implemented.

DER.3.2.A20 Following Up on the On-Site Audit [IS Audit Team]

After the on-site audit, the information collected SHOULD be consolidated further and analysed. After the evaluation of any additional information and documentation required after the fact, the audited requirements SHOULD be subject to a final evaluation.

DER.3.2.A21 Creation of an IS Audit Report [IS Audit Team]

The IS audit team SHOULD transfer the results obtained into an IS audit report and document them transparently therein. A draft version of the report SHOULD be sent in advance to the

audited organisation. It SHOULD be verified whether the issues established by the IS audit team were correctly recorded.

The audited organisation SHOULD ensure that all persons affected in the organisation are provided with the parts of the IS audit report that are important and necessary for them within an appropriate period. In particular, the contents SHOULD be communicated to the top management, the person in charge of the IS audit, and the CISO.

IS audit reports SHOULD be assigned an appropriate confidentiality rating based on the sensitive information they contain.

Consideration SHOULD be given to having the IS audit team present the results of the IS audit to the top management.

DER.3.2.A22 IS Audit Follow-Up [Chief Information Security Officer (CISO)]

The deviations identified in the IS audit report SHOULD be remedied within a reasonable period of time. The corrective measures to be performed SHOULD be documented along with the respective responsibilities, dates of implementation, and status. The implementation SHOULD be followed up continuously and the implementation status updated.

As a matter of principle, it SHOULD be checked whether additional IS audits are necessary. The person in charge of the IS audit SHOULD adapt both the rough and detailed plans for the IS audit.

Requirement in Case of Increased Protection Needs

Generic suggestions for module DER.3.2 *Audits Based on the BSI “Guideline for IS Audits”* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

DER.3.2.A23 Security Checks on IS Auditors (CI)

If the IS auditors access information that is particularly sensitive, the qualification and trustworthiness of the personnel deployed SHOULD be suitably verified.

If material is considered classified (VSA), the IS auditors SHOULD be subjected to a security check in accordance with the German law on security clearance checks (SÜG). In this regard, the CISO SHOULD involve the Confidentiality Officer or Security Representative of the organisation.

Additional Information

For more information about threats and security safeguards for module DER.3.2 *Audits Based on the BSI “Guideline for IS Audits”*, see the following publications, among others:

[ISKR]	Verbindliche Prüfthemen für die IS-Kurzrevision [Binding audit subject list for IS partial audits]: Federal Office for Information Security (BSI), Version 3, June 2018, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Pruefthemen_IS-Kur
--------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	zrevision-v3_pdf.pdf, last accessed on 07.07.2018
[ISR]	Information Security Audit: A guideline for IS audits based on IT-Grundschutz, Federal Office for Information Security (BSI), Version 3.0, March 2018 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Leitfaden_IS-Revision-v3.pdf , last accessed on 09.05.2018
[RH]	Revisionshandbuch zur Informationssicherheit nach UP Bund (Muster) [Audit Manual for Information Security in line with UP Bund (example): Federal Office for Information Security (BSI), Version 1.0, July 2008, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ISRevision/Muster_ISRevisionshandbuch-v1_pdf.pdf , last accessed on 15.08.2018
[VSA]	Allgemeine Verwaltungsvorschrift des Bundesministerium des Inneren zum materiellen und organisatorischen Schutz von Verschlusssachen (VS-Anweisung - VSA) [General Administrative Instructions for the physical and organisational protection of classified material (Classified Material Instructions – VSA)]: Federal Ministry of the Interior (BMI), 01.09.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module DER.3.2 *Audits Based on the BSI “Guideline for IS Audits”*:

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.18	G 0.19	G 0.27	G 0.29	G 0.46
DER.3.2.A1	X		X		
DER.3.2.A2	X				
DER.3.2.A3	X				
DER.3.2.A4	X			X	
DER.3.2.A5	X		X		
DER.3.2.A6	X				
DER.3.2.A7	X				
DER.3.2.A8	X			X	X
DER.3.2.A9	X				
DER.3.2.A10	X	X			X
DER.3.2.A11	X				
DER.3.2.A12	X				
DER.3.2.A13	X				
DER.3.2.A14	X			X	
DER.3.2.A15	X				
DER.3.2.A16	X				
DER.3.2.A17	X				X
DER.3.2.A18	X				
DER.3.2.A19	X			X	
DER.3.2.A20	X				
DER.3.2.A21	X			X	X

DER.3.2.A22	X				
DER.3.2.A23	X			X	X



DER.4: Business Continuity Management

Description

Introduction

In emergency situations, access to information is indispensable for restoring a business process, an IT system or a specialised task. The corresponding processes designed to maintain information security in case of an emergency should thus be planned, established and checked.

Only by following a planned and organised approach can optimal contingency planning and emergency response be achieved. A professional process for business continuity management reduces the impact of emergencies and thereby ensures operations and the continued existence of the organisation. Appropriate safeguards must be identified and implemented to make business processes and specialised tasks more robust and more fail-safe, and to quickly and systematically handle the emergency situation.

That is why the maintenance of information security is to be integrated into comprehensive business continuity management. However, business continuity management has its own process owner (the BCM Officer), who coordinates with the Chief Information Security Officer.

Objective

The aim of module DER.4 *Business Continuity Management* is to describe requirements for ensuring information security even in critical situations. To this end, corresponding safeguards must be embedded into holistic continuity management. Furthermore, all aspects required for maintaining information security in the event of damage must be considered. This includes anything from planning to the checking of all processes.

Not in Scope

In the event of damage, the correct information must be fully available. The present module does not address criteria or processes used by persons in charge to decide whether an emergency has occurred. The decision on this will be made whilst handling the security incident (see DER.2.1 *Security Incident Handling*).

Crises are considered within the scope of in-house crisis management and only addressed as an interface in this module (e.g. within the scope of further escalation of emergencies). Further information on the individual phases of business continuity management and on the differentiation between business continuity management and crisis management are included in BSI Standard 100-4.

Threat Landscape

For module DER.4 *Business Continuity Management*, the following specific threats and vulnerabilities are of particular importance:

Shortage of Personnel

If employees are absent, (e.g. due to germs in the canteen, a pandemic, death, or a strike), the organisation may no longer be able to perform its specialised tasks and business processes. Furthermore, relevant information for restarting the business processes or IT systems may no longer be accessible. In many cases, individual persons have exclusive expert knowledge. As a result, damage may be caused even if the personnel shortage is minimal.

Failure of IT Systems

If components of an IT system fail (e.g. due to defective hardware or power failure), the entire IT operation can be disrupted. This threatens the availability of the relevant information, and thus of the relevant business processes, as well. Furthermore, important information required for restoration measures may be unavailable.

Failure of a Wide Area Network (WAN)

A wide-area network (WAN) can fail for a variety of reasons. It is thus possible that a WAN failure will only affect individual users, a particular provider, or a certain region. Such failures are often short and only affect the business processes and specialised tasks that require high WAN availability. Increasingly, however, long-lasting failures occur and may result in massive problems in communication and accessibility.

Inability to Use a Building

Buildings may unexpectedly become unusable, such as when they have been destroyed partially or completely due to a fire, storm, flood, earthquake, or explosion. However, a building can also be rendered unusable by barriers set up by the police or fire brigade that make it impossible to access the area, or by the necessity to leave the building because the electricity, water, waste water, heating or air conditioning is not working properly.

Failure of or Disruption to a Supplier or Service Provider

If organisational units depend on service providers, the partial or full failure of or disruption to an outsourcing service provider or a supplier may have a major effect on business continuity, and especially on critical business processes.

Requirements

The specific requirements of module DER.4 *Business Continuity Management* are listed below. As a matter of principle, the BCM Officer is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	BCM Officer
---------------------	-------------

Further Roles	Head of Personnel, Chief Information Security Officer (CISO), BCM Officer, Top Management, Supervisor

Basic Requirements

For module DER.4 *Business Continuity Management*, there are no Basic Requirements.

Standard Requirements

For module DER.4 *Business Continuity Management*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

DER.4.A1 Drawing Up a Business Continuity Handbook [Chief Information Security Officer (CISO)]

A business continuity handbook containing the most important information on the following SHOULD be drawn up:

- roles
- immediate measures
- alarming and escalation
- communication plans, basic business continuity plans, restoration plans
- recovery plans

Responsibilities and competences SHOULD be assigned, communicated and recorded in the business continuity handbook. It SHOULD be ensured that appropriately trained personnel are available in emergencies. Tests and exercises SHOULD be performed regularly to check that the safeguards described in the business continuity handbook work as intended.

The business continuity handbook SHOULD be reviewed and, if needed, updated regularly. It SHOULD be accessible in an emergency. In addition, the business continuity handbook SHOULD include rules of behaviour in certain situations (e.g. fire) that should be communicated to all employees.

DER.4.A2 Integrating Business Continuity Management into Organisation-Wide Procedures and Processes [Top Management] (CIA)

The processes in security management SHOULD be coordinated with business continuity management (see DER.2.1 *Security Incident Handling*).

Requirements in Case of Increased Protection Needs

Generic suggestions for module DER.4 *Business Continuity Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is per-

formed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

DER.4.A3 Specifying the Scope and the Business Continuity Strategy [Top Management] (CIA)

The scope of the business continuity management system SHOULD be clearly specified. The organisation's top management SHOULD specify a business continuity strategy that states the goals to be reached and the level of risk considered acceptable.

DER.4.A4 Policy for Business Continuity Management and Acceptance of Overall Responsibility by Top Management [Top Management] (CIA)

Top management SHOULD approve a business continuity policy. This SHOULD include the essential points of business continuity management. The business continuity policy SHOULD be checked regularly and revised when necessary. The business continuity policy SHOULD be communicated to all employees.

DER.4.A5 Establishing a Suitable Organisational Structure for Business Continuity Management [Top Management] (CIA)

The roles for business continuity management SHOULD be specified in accordance with the conditions of the organisation. This SHOULD be documented in writing together with the tasks, obligations and competencies of the roles. Qualified employees SHOULD be appointed to all roles in business continuity management at an organisation. It SHOULD be checked regularly that the organisational structure in business continuity management is effective, efficient, and suitable for practical use.

DER.4.A6 Providing Adequate Resources for Business Continuity Management [Top Management] (CIA)

The financial, technical and personnel resources provided SHOULD be sufficient to reach the intended goals of business continuity management at an organisation. The BCM Officer and the members of the business continuity management team SHOULD have enough time available to perform their tasks in business continuity management at an organisation.

DER.4.A7 Creating a Contingency Concept [Top Management] (CIA)

All critical business processes and resources SHOULD be identified (e.g. using a business impact analysis (BIA)). The most important and relevant risks for critical business processes and resources SHOULD be identified. The risk strategies to be used to treat risks SHOULD be specified for each identified risk. An organisation SHOULD develop continuity strategies that enable the critical business processes to be restored and restarted within the required time. A contingency concept SHOULD be drawn up. Organisations SHOULD develop and implement contingency plans and safeguards that enable an effective emergency response and quick recovery of the critical business processes. The contingency concept SHOULD take into account information security. In turn, the corresponding security concepts SHOULD be developed within this concept for the business continuity solutions.

DER.4.A8 Integrating Employees into the Business Continuity Management Process [Supervisor, Head of Personnel] (CIA)

All employees SHOULD receive regular appropriate awareness training with respect to business continuity management. There SHOULD be a training and awareness-raising concept for

business continuity management. The employees in the business continuity management team SHOULD be regularly trained in the required skills and knowledge.

DER.4.A9 Integrating Business Continuity Management into Organisation-Wide Procedures and Processes [Top Management] (CIA)

It SHOULD be ensured that business continuity aspects are taken into account in all business processes of the organisation. The processes, requirements and responsibilities in business continuity SHOULD be coordinated with risk management and crisis management.

DER.4.A10 Tests and Emergency Drills [Top Management] (CIA)

A drill plan SHOULD be drawn up. It SHOULD ensure that all significant business continuity plans and safeguards are tested and drilled on a regular basis and for specific events. Business continuity management SHOULD have adequate resources available for planning, conception, execution and assessment of tests and drills.

DER.4.A11 Verification and Maintenance of Measures for Contingency Planning and Response (CIA)

The identified measures for contingency planning and response SHOULD be examined on a regular basis and for specific events. These examinations SHOULD be planned so that no relevant parts are skipped. The results of the examinations SHOULD be evaluated and implemented as corrective measures as appropriate. The corrective measures SHOULD be planned and their implementation SHOULD be monitored.

DER.4.A12 Documentation in the Business Continuity Management Process (CIA)

The sequence of events in the business continuity management process, the results of the work done in each of the phases and all major decisions SHOULD be documented. A procedure designed to ensure that documents are updated regularly SHOULD be established. Furthermore, access to the documentation SHOULD be limited to authorised persons only.

DER.4.A13 Checking and Controlling the Business Continuity Management System [Top Management] (CIA)

Top management SHOULD examine, evaluate and, if necessary, correct the business continuity management system on a regular basis. Management reports SHOULD be used to regularly inform top management on the status of business continuity management at the organisation.

DER.4.A14 Regular Checking and Improvement of Business Continuity Safeguards [BCM Officer, Top Management] (IA)

All business continuity safeguards SHOULD be checked regularly, and in case of major changes, to ensure that the defined targets continue to be met and that the safeguards are properly implemented and remain suitable.

Here, it SHOULD be checked that technical safeguards are implemented and configured correctly, and that organisational safeguards are implemented effectively and efficiently. In case of deviations, the causes of defects SHOULD be identified and measures for improvement SHOULD be initiated. Top management SHOULD approve the summary of results. Furthermore, a process that controls and monitors whether and how measures for improvement are implemented SHOULD be initiated. Any delays SHOULD be escalated to top management at an early stage.

The organisation's top management SHOULD specify how to coordinate the examination activities. In particular, the examinations performed in the area of auditing, IT, security management, information security management and business continuity management should be coordinated with each other. To this end, regulations SHOULD be in place to define who examines which safeguards and when.

DER.4.A15 Assessing the Performance of the Business Continuity Management System [Top Management] (IA)

The performance and effectiveness of the business continuity management system SHOULD be assessed regularly. Measurement and evaluation criteria, such as key performance indicators, SHOULD be defined as a basis. Such measurements SHOULD be determined regularly and compared to the values of the previous year. If the values deviate in a negative way, the causes SHOULD be identified and measures for improvement SHOULD be defined. The results of the assessment SHOULD be reported to the management.

Top management SHOULD define the safeguards for further development of business continuity management. All decisions at top management SHOULD be documented, and the previous records SHOULD be updated.

DER.4.A16 Contingency Planning and Emergency Response Planning for Outsourced Components [Top Management] (IA)

In the context of contingency planning and emergency response planning for outsourced components, business continuity management at the supplier or service provider SHOULD be checked in the signed contracts. Such checks SHOULD be performed regularly by a person in charge at top management level. The processes for business continuity tests and drills SHOULD also be coordinated and, if applicable, performed together with the supplier or outsourcing service provider.

The results and assessments SHOULD be exchanged regularly between the organisation's top management and the supplier or service provider. These SHOULD also include any possible measures for improvement.

Additional Information

For more information about threats and security safeguards for module DER.4 *Business Continuity Management*, see the following publications, among others:

[22301]	ISO 22301:2012: Societal security - Business continuity management systems - Requirements, International Organization for Standardization (ed.), ISO/TC 292, May 2012
[27001A17]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, especially Annex A, A.17 Information security aspects of business continuity management, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[27031]	ISO/IEC 27031:2011: Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, March 2011
[BSI3]	Risk Analysis Based on IT-Grundschutz, BSI Standard 200-3, Version 1.0, October 2017,

	https://www.bsi.bund.de/grundschutz
[BSI4]	Business Continuity Management, BSI Standard 100-4, Version 1.0, November 2008, https://www.bsi.bund.de/grundschutz
[BWV]	Modell eines Risikomanagements für die Bundesverwaltung [A Risk Management Model for the Federal Administration]: Report of the Federal Performance Commissioner, Bundesrechnungshof (BRH), April 2017, https://www.bundesrechnungshof.de/de/veroeffentlichungen/gutachten-berichte-bwv/berichte/sammlung/2017-bwv-bericht-modell-eines-risikomanagements-fuer-die-bundesverwaltung , last accessed on 05.10.2018
[ISFBC]	The Standard of Good Practice for Information Security : Area BC Business Continuity, Information Security Forum (ISF), June 2018
[LFKK]	Krisenkommunikation - Leitfaden für Behörden und Unternehmen [Crisis Communication - Guidelines for Authorities and Companies]: Federal Ministry of the Interior, Building and Community (BMI), 5 th edition, August 2014, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/leitfaden-krisenkommunikation.pdf , last accessed on 05.10.2018
[LFKRITIS]	Schutz kritischer Infrastrukturen - Risiko- und Krisenmanagement (Leitfaden für Unternehmen und Behörden) [Critical Infrastructure Protection - Risk and Crisis Management (Guide for Businesses and Authorities): Federal Ministry of the Interior, Building and Community (BMI), May 2011, https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis-leitfaden.html , last accessed on 05.10.2018
[NIST80034]	Contingency Planning Guide for Federal Information Systems: NIST Special Publication 800-34, Revision 1, May 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nist-specialpublication800-34r1.pdf , last accessed on 05.10.2018
[UMRA]	Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4 [Implementation Framework for BSI Standard 100-4]: Federal Office for Information Security (BSI), https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Umsetzungsrahmenwerk/umra.html , last accessed on 05.10.2018
[WKN]	Webkurs Notfallmanagement nach BSI-Standard 100-4 [Web Course on Business Continuity Management according to BSI Standard 100-4]: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/Webkurs1004_node.html , last accessed on 05.05.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module DER.4 *Business Continuity Management*:

G 0.18 Poor Planning or Lack of Adaptation

G 0.27 Lack of Resources

G 0.33 Shortage of Personnel

Elementary Threats Requirements	G 0.18	G 0.27	G 0.33
DER.4.A1	X	X	X
DER.4.A2	X		
DER.4.A3	X		
DER.4.A4	X		
DER.4.A5	X		
DER.4.A6	X	X	X
DER.4.A7	X		
DER.4.A8	X	X	X
DER.4.A9	X	X	
DER.4.A10	X		
DER.4.A11	X		
DER.4.A12	X	X	X
DER.4.A13	X		
DER.4.A14	X		
DER.4.A15	X		
DER.4.A16	X		



APP.1.1: Office Products

Description

Introduction

The group of Office products comprises all applications that are used to create, edit, and view documents. Among other things, they include the free LibreOffice application and the proprietary Microsoft Office application used in many organisations. Office products are part of the basic IT tools most organisations need. Among other things, they comprise word processing, spreadsheets, presentation creation, and drawing programs, as well as simple database systems. Office applications make it possible to obtain and process information.

Objective

The objective of the present module is to protect the information processed and used when using Office products. For this, there are special requirements regarding the mode of operation of the components of Office products. The module illustrates requirements that should be implemented in order to protect Office products against specific threats.

Not in Scope

This module considers the use of Office products from the perspective of an IT Operation Department and provides information for users as to how Office products should be used. Specific requirements are included that must be taken into account when using Office products. As a complement to the requirements of this module, it must be ensured that the requirements of the generic module CON.4 *Selection and Use of Standard Software* are implemented. E-mail and PIM applications are not covered in this module; the corresponding requirements are documented in the module APP.5.1 *General Groupware*. For Microsoft e-mail and PIM applications, module APP.5.2 *Microsoft Exchange and Outlook* must also be considered. When using integrated database systems such as Base in LibreOffice or Access in Microsoft Office, the module APP.4.3 *Relational Database Systems* must be considered. The present module does not include any pure cloud office applications either, such as Google's G Suite (Docs, Sheets, etc). Requirements regarding cloud applications are defined in the modules OPS.2.2 *Cloud Usage* and APP.5.3 *Cloud Applications from a Client Perspective*.

Threat Landscape

For module APP.1.1 *Office Products*, the following specific threats and vulnerabilities are of particular importance:

Poor adaptation of the Office products to the requirements of the organisation

If requirements for Office products are not considered when procuring or adapting the software, operations may be disrupted significantly. The reasons for this may include, for example, a lack of compatibility with existing templates and documents, an insufficient scope of functions in the version used, or a lack of interoperability with applications used by business partners. If Office products are not adapted to the requirements of the organisation, this may cause reduced performance, failures, and errors within business processes.

Non-Existent or Inadequate Testing and Approval Procedures Regarding Office Products

If new Office products and their integration into the organisation are inadequately tested or not tested at all and then approved without any installation instructions, errors may remain undetected or necessary installation parameters may not be taken into consideration. Errors in Office products resulting from non-existent or inadequate testing and approval procedures pose a significant threat to IT operations. Procedures may be hindered significantly due to Office product errors. Erroneous updates of Office products may cause data losses or limit the availability of databases used.

Sensitive Data in Residual Information in Office Documents

Office documents normally contain meta information on the document itself, as well as information on the author and the organisation. Any number of user-defined entries can be added to this meta information to support the procedures of business processes and provide for an appropriate level of transparency. Additionally, Office products provide the option to create comments within the document and add or change information in review mode. This and additional residual information may include confidential information that must not be made accessible to third parties. Otherwise, this may lead to a loss of confidentiality and the falsification of the residual information at a later point in time, which in turn can result in financial, process-related, and reputational damage.

Procurement of Office Products and Updates from a Reliable Source

If installation sources or updates of Office products are procured from unofficial sources, there is no guarantee that the software will work properly and not contain malicious code. This applies both to the Office products themselves and to the functions present as a plug-in, add-on or macro in documents. This may result in calculations arriving at incorrect results or the integrity and availability of systems being impaired.

Manipulation of Office Documents

The manipulation of Office documents refers to changes made to the information they contain. In many cases, Office documents can include different “active content”, which is sometimes used for complex automation processes. However, active content may also include malicious code that is executed with the rights of the user when the document is opened. Along with manipulating the corresponding document, such malware in Office documents may modify additional documents without this being recognised or insert itself into additional documents. This may impair or block the functions of all the business processes affected at the organisation. In the worst case, the manipulation remains undetected, resulting in vulnerabilities and the processing of falsified information.

Lack of Reliability of Office Documents

Depending on the purpose at hand, it may be necessary to reliably assign Office documents to one or several authors or demonstrate that someone has taken note of a document. If this feature can be bypassed easily, does not meet the relevant legal requirements, or has simply not been considered at all, this can result in invalid contracts or the legitimacy of existing contracts being disputed.

Loss of Integrity of Office Documents

The integrity of Office documents may be falsified due to accidental changes or wilful manipulations of the documents' content. When Office products are handled carelessly or users do not know how to handle Office documents, undetected changes may be made to the documents. This is particularly problematic if the documents are used in production environments. If documents that have been falsified without this being recognised continue to be used, improper business-related decisions may be made or the organisation's image may be damaged.

Software Vulnerabilities in Office Products

Despite comprehensive testing, software vulnerabilities in Office products are often not detected completely prior to their being delivered to customers. If these software vulnerabilities are not detected in time, system crashes and application errors may be the result. The consequences of errors that have not been remedied may include incorrect calculations or a loss of document integrity. Furthermore, software vulnerabilities and errors may cause serious security gaps in Office products. These may be exploited by attackers in order to plant malicious code.

Use of Unlicensed Office Products

Unlicensed Office products are a possible financial security threat for organisations. If Office products without a valid software licence are being used – for example, because the licence volume has been exceeded – this can result in penalties. On the other hand, the licence costs being paid may be too high if Office products are installed on workstations where they are not needed.

Data Loss Due to Password-Protected Office Documents

Data losses in Office documents may block business processes. Normally, Office products provide the option to protect a document with a password when saving it. The password will then be required to open or edit the document. If this feature is used carelessly, assigned document passwords may be forgotten or lost. This can make it impossible to read important documents or edit them further without increased effort. The resulting added effort must be compensated in technical and organisational terms, which in turn leads to increased workloads.

Prohibited Misuse of Rights in Office Products

Access rights are used as organisational safeguards to ensure that information, business processes, and IT systems are protected against unauthorised access. If unauthorised persons may access Office products as a consequence of improperly set authorisations, this may endanger the confidentiality and integrity of information by exposing it to changes, deletion, and improper creation. These vulnerabilities are typically caused by improperly assigned rights. Affected business processes can be corrupted, incorrect information can be processed accidentally and sensitive information can be disclosed.

Requirements

The specific requirements of module APP.1.1 *Office Products* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept defined. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User

Basic Requirements

For module APP.1.1 *Office Products*, the following requirements **MUST** be implemented as a matter of priority:

APP.1.1.A1 Ensuring the Integrity of Office Products

When installing Office products, it **MUST** be ensured that only original, unmodified copies of approved software are being used. Updates **MUST** only be taken from secure sources. If checksums are provided for an Office product, they **SHOULD** be verified prior to installation. If digital signatures are available for an Office product, the signatures **SHOULD** be checked prior to installing the package. The administrators **SHOULD** be informed of the importance and validity of checksums and digital signatures. Like during a new installation, it **MUST** be ensured when installing updates that the update packages have not been changed.

APP.1.1.A2 Limiting Active Content [User]

The automatic execution of embedded active content such as macros or ActiveX elements **MUST** be disabled in the settings of all the Office products used. If it is necessary for a business process to execute active content, it **MUST** be ensured that only active content from trustworthy sources is being executed. The awareness of all users regarding the threats posed by active content **MUST** be raised in training measures, and all users **MUST** be instructed regarding the features for limiting active content.

APP.1.1.A3 Opening Documents from External Sources

All documents from external sources **MUST** be checked for malware before they are opened. All file formats considered problematic and those not required within the organisation **MUST** be prohibited. Users' awareness of how to handle documents from external sources **MUST** be raised, and they **MUST** be trained in this regard. Technical safeguards **SHOULD** be implemented to ensure that documents from external sources are checked.

APP.1.1.A4 Ensuring Ongoing Operations of Office Products

The IT Operation Department and CISO **MUST** regularly obtain information on vulnerabilities that have come to light in Office products. Existing patches **MUST** be installed in a timely manner.

The users SHOULD be informed about the capabilities and limits of the security functions of the software employed and the storage formats used. The specifications for making secure use of Office products SHOULD be integrated into the security policy.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module APP.1.1 *Office Products*. They SHOULD be implemented as a matter of principle.

APP.1.1.A5 Selecting Suitable Office Products

Within the context of procuring Office applications, the requirements of the organisation regarding such products SHOULD be ascertained by the IT Operation Department and the particular department in question. They should be documented in a requirements catalogue. Once all requirements regarding the Office product to be procured have been documented, the products available on the market SHOULD be examined in order to determine the extent to which they fulfil the requirements of the organisation. When choosing from several alternatives, additional effort SHOULD be taken into consideration as well; this includes, for example, the effort required for training measures for administrators and users and for migration.

APP.1.1.A6 Testing New Versions of Office Products

New versions of Office products SHOULD be tested regarding their compatibility with the organisation's established equipment (e.g. document templates, forms) prior to being used in production environments. To this end, methods SHOULD be developed and approved for the individual tests (test types, processes and tools). It SHOULD be ensured that important equipment will continue to function as it should with the new software features provided. If compatibility issues are detected, a migration plan for the documents affected SHOULD be drawn up.

APP.1.1.A7 Installation and Configuration of Office Products

A standard configuration adapted to the requirements of the organisation SHOULD be drawn up and applied to the Office products in use. This configuration SHOULD be documented in installation and configuration instructions. Installation and configuration SHOULD be performed according to the instructions, including with regard to the application of the standard settings. Any necessary deviations from the defined standard configuration SHOULD be documented comprehensibly and require the approval of an appropriate body. Pilot installations SHOULD always be supported by the IT Operation Department. Prior to and after installation, backups of Office products SHOULD be performed on all the relevant IT systems.

APP.1.1.A8 Version Control for Office Products

The installed versions of Office products SHOULD be checked at regular intervals. A corresponding inventory of software licences SHOULD be updated following every installation or uninstallation. Furthermore, the various configurations of installed Office products SHOULD be documented.

APP.1.1.A9 Deletion of Residual Information Prior to Forwarding Documents [User]

Prior to forwarding documents to third parties, all unnecessary and confidential residual information SHOULD be deleted from Office documents. Additionally, the metadata SHOULD be deleted. The awareness of all users regarding the risks caused by residual information and ways to delete it in the Office products used SHOULD be raised, and all users SHOULD be trained in this regard. Documents SHOULD be transmitted in a non-editable format if they do not require editing by the recipient.

APP.1.1.A10 Regulations for Software Development by End Users [User]

Binding regulations on software developed by end users based on Office applications (e.g. macros, table calculations) SHOULD be stipulated; see also APP.1.1.A2 *Limiting Active Content*. First, every organisation SHOULD make a policy decision as to whether or not it wants to allow custom developments of this kind. The decision SHOULD be documented in the corresponding security policies. If custom developments are permitted, a process for handling corresponding features of the Office products SHOULD be developed for the end users. Responsibilities SHOULD be clearly defined. All information pertaining to the applications created SHOULD be documented. Current versions SHOULD be made available to all users affected in a timely manner.

APP.1.1.A11 Controlled Use of Extensions for Office Products

All extensions for Office products SHOULD be tested prior to being used in production environments (as in the process of testing new versions). The tests to be performed SHOULD only be performed on isolated test systems. The tests SHOULD ensure that extensions do not have any adverse consequences for the Office products or IT systems in operation. The tests of the extensions used SHOULD follow a defined test schedule that can be understood by third parties.

APP.1.1.A12 No Cloud Storage [User]

The cloud storage features integrated into some Office products SHOULD be disabled as a matter of principle. All cloud drives SHOULD be disabled. All documents SHOULD be stored on file servers centrally administrated by the organisation. In order to approve documents for viewing or editing by third parties, specialised means (appropriate data rooms, for example) SHOULD be used that have security features such as encrypted data storage and transmission and an appropriate system for user and rights management.

APP.1.1.A13 Use of Viewer Features [User]

Data from potentially insecure sources such as the Internet or e-mail attachments SHOULD automatically be opened in a protected mode where immediate editing is not possible. Only general navigation SHOULD be allowed. The user SHOULD NOT be allowed to disable this feature. Corresponding viewer applications SHOULD be used, if available. A list of trustworthy places from which content can be opened and edited directly can be defined.

APP.1.1.A14 Protection Against Subsequent Changes to Information [User]

Depending on the desired purpose of documents, the security mechanisms in application programs SHOULD be used in order to limit further handling of the created files. The employees SHOULD be made aware of how these security mechanisms work and how they are to be applied.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.1.1 *Office Products* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.1.1.A15 Use of Encryption and Digital Signatures (CI)

Data with increased protection needs SHOULD be encrypted prior to being transmitted or stored in order to ensure confidentiality. Prior to using an encryption process integrated into an Office product, it SHOULD be examined whether this process provides for sufficient protection; this is particularly applicable to earlier product versions. The IT systems of the sender and receiver SHOULD guarantee access protection regarding the method used for encryption. Users' awareness of how to handle the encryption features SHOULD be raised, and they SHOULD be trained in this regard. In addition, a process SHOULD be used that supports the digital signing of macros and documents. The validity of the certificates used SHOULD be limited in terms of time.

APP.1.1.A16 Checking Document Integrity (I)

In order to provide protection against accidental changes to data with increased protection needs during transmission and/or storage, checksum processes SHOULD be used. A process SHOULD be selected that is capable of automatically correcting the data. Furthermore, cryptographic checksum processes SHOULD be used in order to protect against manipulation.

Additional Information

For more information about threats and security safeguards for module APP.1.1 *Office Products*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[LIBRE]	LibreOffice: The Document Foundation, https://de.libreoffice.org , last accessed on 06.09.2018
[MSTN]	Microsoft Technet: https://technet.microsoft.com/de-de , last accessed on 06.09.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.1.1 *Office Products*:

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.28	G 0.29	G 0.37	G 0.39	G 0.45	G 0.46
APP.1.1.A1			X	X					X		
APP.1.1.A2		X			X				X		
APP.1.1.A3							X		X		
APP.1.1.A4		X				X			X		X
APP.1.1.A5	X										
APP.1.1.A6	X		X	X		X				X	X
APP.1.1.A7	X		X								
APP.1.1.A8	X						X				
APP.1.1.A9		X									
APP.1.1.A10	X					X					
APP.1.1.A11			X	X		X	X		X	X	
APP.1.1.A12	X	X					X				X
APP.1.1.A13			X			X			X		
APP.1.1.A14		X			X			X			X
APP.1.1.A15		X	X		X			X			X
APP.1.1.A16			X		X				X		X



APP.1.2: Web Browsers

Description

Introduction

Web browsers are application programs that can access (hypertext) documents, images, video, audio and other data formats on the Internet for processing, viewing, output, and storage on local IT systems. Web browsers can transmit data to the Internet, as well. Today, stationary and mobile client systems are unthinkable without web browsers because many private and business applications use corresponding content.

At the same time, online content is becoming more and more diverse. An increasing number of websites rely on embedded videos, animated elements and other active content. State-of-the-art web browsers cover a large spectrum of additional functions by embedding plug-ins and external libraries. Then there are extensions for certain functions, data formats and content. The complexity of state-of-the-art web browsers also comes with significant potential for serious design errors and technical vulnerabilities. It increases possible risks pertaining not only to attacks from the Internet, but programming and operating errors, as well.

The consequences regarding data confidentiality and integrity are significant. Moreover, such vulnerabilities threaten the availability of entire IT systems. As a matter of principle, Internet content must thus be considered untrustworthy from a web browser perspective.

Objective

This module describes security requirements for web browsers used on client systems, i.e. on stationary and mobile computers, as well as on some tablets and smartphones. Both centrally managed and individual operating environments are addressed.

Not in Scope

This module includes basic security requirements to be considered and fulfilled when installing and operating web browsers for accessing data from the Internet. This module does not address browsers for accessing only local data or data in internal data networks not connected to the Internet.

Web browsers are closely connected to the operating system of the client system in question and use the interfaces and functions it provides. In order to safeguard operating systems, the requirements of the modules of the layers *SYS.2 Desktop Systems* and *SYS.3.2.1 General Smartphones and Tablets* should be fulfilled.

Web applications used with browsers, along with the servers that provide such applications, are addressed in modules *APP.3.1 Web Applications* and *APP.3.2 Web Servers*.

Threat Landscape

For module *APP.1.2 Web Browsers*, the following specific threats and vulnerabilities are of particular importance:

Execution of Malicious Code by Web Browsers

Web browsers can load data from sources that are not trustworthy, or even compromising in nature. Such data may contain executable code that exploits vulnerabilities to infect the device of the user without his or her knowledge.

This may include code (in JavaScript, for example) that can be directly executed by the web browser. It can also be executable code of a plug-in or an extension in connection with the browser, such as Adobe Flash, Java or parts of PDF documents. Finally, code can be loaded by the web browser onto the client and executed there outside of the browser's process. In many cases, the malicious code also loads further malware to be executed on the client with the rights of the user. If the basic protection mechanisms of state-of-the-art web browsers are not used sufficiently, the confidentiality, integrity and availability of information or services on the client side or in any connected networks will be threatened.

Exploit Kits

Lists of vulnerabilities and so-called exploit kits make it significantly easier to develop custom malware. Cyber attacks can be automated in order to use drive-by downloads or other methods of distribution by simple means that require no expert knowledge. Attackers may exploit known vulnerabilities of the web browser or a connected resource or extension to prepare subsequent attacks or load and install malicious code on the client.

Eavesdropping on Internet Communications

The basic security of communication on the Internet significantly depends on the authentication methods used and the encryption of data during transmission. The required methods are often poorly implemented.

Weak implementation of the necessary methods is very common, and it prevents effective authentication and encryption. Many web services still use outdated encryption methods. As a result, attackers can bypass server authentication techniques, and communications or data may not be sufficiently encrypted. This may allow unauthorised individuals to access or modify information as it is being transmitted. In the past, certification bodies have also been compromised, opening the door for attackers to obtain certificates for third-party websites.

Loss of Web Browser Integrity

If browsers, plug-ins or extensions are obtained from untrustworthy sources, malicious functions may be executed inadvertently without being noticed. For example, attackers may falsify components such as the toolbars of web browsers to lure users to manipulated copies of web pages that are used for phishing attacks. Malicious extensions may manipulate the content of viewed web pages or collect data and send it to the attacker.

Loss of Privacy

If browsers are not securely configured, trustworthy data can be disclosed to unauthorised third parties in an inadvertent or wilful manner. Passwords may also be unintentionally for-

warded. If cookies, passwords, histories, entry data and search requests are stored or unnecessary extensions are activated, it will be easier for third parties or malware to read data in order to misuse it.

Administrative and Operating Errors

Errors in web browser administration may result in insecure configurations and operations. A web browser that is not sufficiently updated or maintained is a significant potential threat. Browser providers often fail to offer security updates promptly. This significantly increases the distribution rate of exploitable vulnerabilities.

Requirements

The specific requirements of module APP.1.2 *Web Browsers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept defined. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User

Basic Requirements

For module APP.1.2 *Web Browsers*, the following requirements **MUST** be implemented as a matter of priority:

APP.1.2.A1 Using Sandboxing

The web browser used **MUST** ensure that every instance and every process can only access its own resources (sandboxing). Web pages **MUST** be isolated from each other as independent processes, or at least in their own threads. Plug-ins and extensions **MUST** also be executed in isolated areas. The web browser used **SHOULD** implement the W3C's Content Security Policy.

APP.1.2.A2 Encryption of Communications

The web browser **MUST** support a secure version of Transport Layer Security (TLS). Insecure versions of TLS **SHOULD** be deactivated. The web browser **MUST** support the HTTP Strict Transport Security (HSTS) security mechanism according to RFC 6797. The domains **SHOULD** be inserted into the HSTS preload list of the browser for all important public TLS-encrypted web services.

APP.1.2.A3 Using Certificates [User]

The web browser **MUST** provide a list of trustworthy root certificate issuers and accept the certificates provided by the organisation itself. The web browser **MUST** support Extended Validation certificates. Root certificates **MUST ONLY** be added, changed or deleted with administration rights. It **MUST** be possible to withdraw certificates (locally) through the web browser.

The web browser **MUST** check the validity of the server certificates completely using the public key and the validity period. The web browser **MUST** verify the lock status of the server certificates. The certificate chain, including the root certificate, **MUST** be verified.

The web browser **MUST** indicate to the user in a clear and well noticeable manner that communication is taking place in plain text or in an encrypted manner. The web browser **SHOULD** be able to show the user the server certificate in use upon request. The web browser **MUST** alert the user when certificates are lacking, invalid or withdrawn. In such cases, the encrypted connection **MUST ONLY** be established after express confirmation by the user.

APP.1.2.A4 Version Checking and Updates for Web Browsers

The web browser **MUST** have a mechanism that is able to reliably detect and display its own version, as well as the versions of all loaded or activated extensions and plug-ins.

Security updates for the web browser, plug-ins and extensions **MUST** be installed immediately. The web browser **SHOULD** be able to automatically install updates. If no update is available for a known critical vulnerability, measures for mitigation **MUST** be taken promptly.

Standard Requirements

For module APP.1.2 *Web Browsers*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

APP.1.2.A5 Basic Configuration

It **SHOULD** be possible to configure the browser centrally. The users **MUST NOT** be able to change centrally provided settings. The web browser **SHOULD NOT** be run with extended rights on a continuing basis.

APP.1.2.A6 Password Management in Web Browsers [User]

If a password manager is used in the browser, it **SHOULD** create a direct and unique relationship between web pages and the passwords stored for them. The stored passwords **SHOULD** be protected. It **SHOULD** only be possible to access the passwords stored in the password manager after entering a master password. Authentication for password-protected access **SHOULD** only be valid for the current session. The password manager **SHOULD** specify a certain level of password quality in accordance with the security policy of the organisation. It **SHOULD** be possible for the user to delete stored passwords.

APP.1.2.A7 Data Protection [User]

Cookies from third parties **SHOULD** be refused. It **SHOULD** be possible for users to delete stored cookies.

The auto-complete function for data **SHOULD** be deactivated. If the function is still used, the user **SHOULD** be able to delete the completion data. The user **SHOULD** also be able to delete the browser's history data.

If available, the browser's synchronisation with cloud services **SHOULD** be deactivated. Telemetry functions and the automatic sending of crash reports to the browser's provider **SHOULD** be deactivated whenever possible.

If peripheral devices such as microphones or webcams are connected, they SHOULD be deactivated in the browser. The browser SHOULD offer a possibility to configure and deactivate WebRTC, HSTS and JavaScript.

APP.1.2.A8 Using Plug-ins and Extensions [User]

Only absolutely necessary plug-ins and extensions SHOULD be installed. Updates SHOULD only be obtained from trustworthy sources. Administrative rights SHOULD be required to install plug-ins and extensions for the browser. The execution of plug-ins SHOULD always require confirmation by the user. The browser SHOULD offer the possibility to configure and deactivate extensions.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.1.2 *Web Browsers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.1.2.A9 Using an Isolated Browser Environment (CI)

In case of increased protection needs, web browsers running in an isolated environment (like ReCoBS) or on dedicated IT systems SHOULD be used.

APP.1.2.A10 Using Private Mode [User]

In case of increased requirements regarding confidentiality, the browser SHOULD be run in private mode so that no information or content will be stored persistently on the user's IT system. The browser SHOULD be configured so that local content will be deleted once the browser is closed.

APP.1.2.A11 Checking for Malicious Content (C)

The browser SHOULD check the Internet addresses accessed by the user for potentially malicious content. The browser SHOULD provide a suitable warning to the user if information on malicious content is present. It SHOULD NOT be possible to establish a connection that is classified as malicious. The procedure used for checking MUST NOT infringe on provisions of data protection or the protection of classified information.

APP.1.2.A12 Two-Browser Strategy (A)

If the browser in use has unsolved security problems, an additional browser from another provider SHOULD be installed as a substitute.

Additional Information

For more information about threats and security safeguards for module APP.1.2 *Web Browsers*, see the following publications, among others:

[AbWeB]	Absicherungsmöglichkeiten beim Einsatz von Web-Browsern [Security options when using Web browsers]: BSI Publications on Cyber Security (BSI-CS 047), Version 1.0, January 2013, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_047.pdf , last accessed on 11.09.2018
---------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[ACSDB]	SSL Cipher Suite Details of Your Browser: University of Hanover, https://cc.dcsec.uni-hannover.de , last accessed on 11.09.2018
[CSP]	Content Security Policy 1.0: W3C Candidate Recommendation, W3C, November 2012 https://www.w3.org/TR/2012/CR-CSP-20121115/ , last accessed on 11.09.2018
[HSTS]	HTTP Strict Security Policy (HSTS): RFC 6797, Internet Engineering Task Force (IETF), November 2012, https://tools.ietf.org/html/rfc6797 , last accessed on 11.09.2018
[MDST8SSL]	Mindeststandard des BSI für den Einsatz des SSL/ TLS-Protokoll durch Bundesbehörden nach § 8 Abs. 1 Satz 1 BSIG [BSI minimum standard for the use of the SSL/TLS protocol by federal authorities according to Section 8(1) Sentence 1 of the BSIG]: Federal Office for Information Security (BSI), Version 1.0, February 2015 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf , last accessed on 11.09.2018
[MDST8Web]	Mindeststandard des BSI für sichere Web-Browser nach § 8 Absatz 1 Satz 1 BSIG [BSI minimum standard for secure web browsers according to Section 8(1) Sentence 1 of the BSIG]: Federal Office for Information Security (BSI), Version 1.0, March 2017, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Sichere_Web-Browser.pdf , last accessed on 11.09.2018
[OWASPList]	OWASP List of the 10 Most Critical Web Application Security Risks: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project , last accessed on 11.09.2018
[ReCoBS]	Common Criteria Protection Profile for Remote-Controlled Browsers System (Re-CoBS): BSI-PP-0040, Federal Office for Information Security (BSI), Version 1.0, February 2008, https://www.commoncriteriaportal.org/files/ppfiles/pp0040b.pdf , last accessed on 11.09.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.1.2 *Web Browsers*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.39 Malware

G 0.40 Denial of Service

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0.1 4	G 0.1 5	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 5	G 0.2 6	G 0.2 8	G 0.3 0	G 0.3 1	G 0.3 9	G 0.4 0	G 0.4 5	G 0.4 6
Requirements																	
APP.1.2.A1				X				X			X			X			
APP.1.2.A2	X		X	X			X										X
APP.1.2.A3	X		X		X		X										X
APP.1.2.A4					X	X		X		X	X			X			
APP.1.2.A5			X			X						X	X				
APP.1.2.A6			X	X								X	X				
APP.1.2.A7	X	X		X								X	X			X	
APP.1.2.A8			X				X				X	X	X				
APP.1.2.A9								X		X	X			X			
APP.1.2.A10	X			X													
APP.1.2.A11								X			X						
APP.1.2.A12			X						X	X	X				X		



APP.1.4: Mobile Applications (Apps)

Description

Introduction

Smartphones, tablets and similar devices are widely used today in public authorities and companies, where they enable employees to access an organisation's data, information and applications whenever and wherever required.

Mobile applications (also known as applications or "apps" for short) are applications that are installed and executed on mobile operating systems such as iOS or Android on corresponding end devices. Apps are usually obtained from app stores, which are operated and maintained by the manufacturers of the mobile operating systems and end devices. In professional environments, however, it is also common for an organisation to develop its own apps and install and manage them on end devices using MDM solutions. Compared to applications on desktop operating systems, iOS or Android apps are subject to special framework conditions, such as the authorisation management ensured by the operating system.

There is now a huge selection of available apps for different mobile operating systems. There are also standardised libraries and development environments that enable apps to be developed quickly compared to classic applications.

Objective

The objective of this module is to protect information that is processed with and by apps on end devices. It also aims to protect information that is processed on mobile devices or IT systems that are networked with them. To these ends, it defines requirements for correctly selecting apps and operating them securely regardless of their source (an app store or in-house installation).

Not in Scope

The module considers apps in mobile operating systems such as iOS and Android. However, requirements concerning the underlying operating systems are not taken into account when considering the security of mobile applications; these can be found, for example, in modules SYS.3.2.3 *iOS (for Enterprise)* and SYS.3.2.4 *Android*. Apps are often centrally managed in a mobile device management system. The requirements for this are covered in module SYS.3.2.2 *Mobile Device Management (MDM)* rather than in this module.

Similarly, the application-specific aspects of apps are not part of this module; these are addressed in the corresponding modules in the APP (applications) layer.

Apps often rely on back-end/server systems or application services. Security recommendations related to this are not provided here and should be obtained from the corresponding modules. These include, for example, APP.3.1 *Web Applications*, APP.3.5 *Web Services* and APP.4.3 *Relational Database Systems*. Modules dealing with general aspects of applications, such as OPS.1.1.6 *Software Tests and Approvals* or CON.4 *Selection and Use of Standard Software*, should also be considered, as these aspects are not covered in this module. The requirements of module CON.8 *Software Development* should be considered in the development of in-house apps.

Threat Landscape

For module APP.1.4 *Mobile Applications*, the following specific threats and vulnerabilities are of particular importance:

Inappropriate Selection of Apps

Selected apps have a strong impact on the information they process and on the organisation's IT infrastructure in general. Failure to consider this when selecting apps can lead to far-reaching problems. The threat is particularly high when dealing with apps that have not been developed specifically for the business processes to be mapped. For example, the prerequisites for operating an app – such as the performance of mobile network connections or compatible hardware – might not be considered sufficiently. In addition, apps may not be suitable if they do not provide sufficient long-term stability and planning or are not adequately maintained by the manufacturer.

Lack of Resources and Skills

Many organisations underestimate how complex it is to use apps in a controlled way. Today's smartphones, tablets and similar mobile devices are powerful IT systems that employees often use for both personal and business purposes. In many organisations, however, the devices and the apps on them are not adequately secured and maintained because they are often still regarded as simple telephones. If an organisation lacks the resources and skills necessary for mobile device administration, apps could be used in an uncontrolled manner, creating security risks for the organisation's information and IT infrastructure.

Insufficient Checking and Auditing Options

If employees install business apps on private end devices, organisations cannot check which apps are being used or where and what data they are transferring. It is also more difficult to correct any errors that may occur, as administrators often have limited access to the devices. For the same reason, it is more difficult to analyse any logging data that may be generated. This allows attackers to manipulate the communication between the app and the organisation's servers undetected, for example, or to access sensitive information.

Excessive Authorisations

iOS and Android apps need certain permissions to access particular functions and services. An app can usually always access the Internet connection of the mobile device, while access to the location or the address book requires separate approval. If apps are used that require authorisations that are too extensive or the authorisations are not sufficiently restricted, this can have particular consequences for the confidentiality and integrity of the information on the end device. Apps can share locations, photos, contact and calendar information, and other data with unauthorised third parties. They can also change or delete local data and generate costs, such as by making telephone calls, sending SMS messages or making in-app purchases.

Undesired Functions in Apps

Although apps are checked by some app store operators, they can still contain vulnerabilities or deliberately malicious functions. The risk is particularly high when apps are obtained and installed from untested or unreliable sources and the confidentiality, integrity and availability of information can be compromised. If apps are no longer updated by the manufacturer to address security vulnerabilities, this has a significant impact on the information processed.

Software Vulnerabilities and Errors in Apps

Apps can contain vulnerabilities that allow attacks on the device either directly or through the network connections. In addition, it is common for developers to stop maintaining their apps after some time, which prevents any detected security deficiencies from being corrected by appropriate updates.

Insecure Storage of Local Application Data

Some apps store data such as documents or user profiles on the end device. If this data is not sufficiently protected, other apps may be able to access it. It can also be easily read by unauthorised persons if an employee loses a device, for example. In addition, locally stored information is often not included in the data backup policy, which means that it cannot be recovered if the end device is lost or fails. In addition to data that has been consciously stored, this also applies to temporary data, such as information stored temporarily in the cache.

Metadata and Inference of Confidential Information

Apps accumulate considerable metadata that can be used to deduce confidential information, such as phone and network connections, location data, or web pages visited. Further information can then be derived from this, such as the structure of an organisation, exact locations and the staff who work there.

Leaks of Confidential Data

Data is transferred to and from an app in different ways. Mobile operating systems provide various interfaces for this purpose and for transferring data between apps. Users also have various options for exchanging data with an app, such as locally via a memory card, using the clipboard or the device camera and other applications. In addition, data can be transferred via cloud services or a server operated by the app or device provider. This may give third parties access to the confidential data. Finally, the operating system itself can also cache data for faster access. This can enable the inadvertent outflow of data or allow attackers to access confidential information.

Insecure Communication with Back-end Systems

Many apps communicate with back-end systems that exchange data with the organisation's data network. In the case of mobile devices, the data is usually transmitted via insecure networks (mobile networks, WLAN hotspots, etc). If insecure protocols are used for communication with back-end systems, information can be intercepted or manipulated.

Interactions with Other Apps

Depending on their authorisations, apps can unintentionally cause disruptions if they change or influence network configurations (such as firewalls or VPN) or block or manipulate required

resources (GPS, audio, camera). They can also interfere with each other through contradictory synchronisations of data (appointments, contact data) or by deleting data from each other.

Communications Channels Beyond the Organisation’s Infrastructure

If apps can communicate in an uncontrolled manner with third parties, this can create communication channels that are not recognised and controlled by the organisation. For example, a user could transfer information from an end device to the outside world through a cloud data storage app. The close integration of social media services with many apps also makes it difficult to check whether and how information leaves the end device in an uncontrolled way. In addition to the lack of traceability of such communication channels, this can also cause problems if, for example, the user or the organisation are obliged to archive information or transactions.

Unmanaged Apps and Unmanaged End Devices

Employees often use their end devices for personal purposes, as well. If the users are able to install apps on mobile devices, the organisation is often unable to check them. Such apps can have vulnerabilities that compromise devices intended for business purposes. Conversely, if a business app is installed on a device that is not under the control of the organisation (such as a private smartphone), confidentiality and integrity may be compromised if the device contains malware, for example.

Dependence on Back-end or External Systems and Services

Many apps depend on external systems and services and offer limited functionality (or none at all) without an active data connection. If the connection to a necessary service or even the service itself fails, the app will no longer work and the information it has processed will not be available. This problem can also occur if the service provider makes changes to the APIs and the app is not updated in time.

Requirements

The specific requirements of the module APP.1.4 *Mobile Applications (Apps)* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Data Protection Officer, User, Process Owner

Basic Requirements

For module APP.1.4 *Mobile Applications (Apps)*, the following requirements **MUST** be implemented as a matter of priority:

APP.1.4.A1 Requirements Analysis for Apps [Process Owner]

Before installing and using an app, there **MUST** be a clear definition of the business processes the app supports and the organisational IT components to which it should be connected. Furthermore, security requirements **MUST** be defined for the app. In addition, the protection needs and the general legal framework conditions relating to the data to be processed **MUST** be considered.

In the requirements analysis, risks arising from mobile use in particular **MUST** be considered. The organisation **MUST** verify that its ability to check and influence the operating system environment of mobile devices is sufficient for secure use.

APP.1.4.A2 Rules Regarding the Use of Mobile Devices and Apps

Since not all security-relevant aspects for mobile end devices can be solved technically, a policy for the use of apps **MUST** be created for employees. At minimum, this policy **MUST** govern the following:

- which data may be processed on the devices (and the extent to which private use is permitted)
- who is authorised to install which apps on the devices
- how users should behave in public data networks
- what to do if a device gets lost

These requirements **MUST** match the established rules of the organisation.

APP.1.4.A3 Secure Sources for Apps [User]

It **MUST** be ensured that apps can only be obtained from secure and trusted sources. **ONLY** trustworthy app stores may be used. Apps developed within the organisation and apps that process sensitive information **SHOULD** be distributed through the organisation's own app store or MDM.

APP.1.4.A4 Testing and Approval of Apps [Data Protection Officer, Process Owner]

It **MUST** be ensured that the app can be integrated into the existing operation and all requirements are met in terms of technical areas, information security and data protection. Before a new app or a new version of an app is used, it **SHOULD** be tested and then expressly approved. Appropriate tests **SHOULD** be developed and approval criteria defined for all areas. The results of the tests **SHOULD** be documented and serve as a basis for the approval of the app. Particular care **SHOULD** be taken to ensure that the tests are performed on all devices and operating system environments used in the organisation, and that the release criteria are met.

APP.1.4.A5 Minimising and Checking App Authorisations [Process Owner]

Before an app is introduced in an organisation, it **MUST** be ensured that it only has the minimum app authorisations required for its function. Authorisations that are not absolutely necessary **MUST** be scrutinised and, if necessary, disabled.

Security-relevant authorisation settings **MUST** be fixed so that they cannot be changed by users or apps. If this is not technically possible, the settings **MUST** be regularly checked and re-set.

APP.1.4.A6 Patch Management for Apps

Updates for apps **MUST** be installed promptly. If the organisation uses a mobile device management (MDM) system, it **MUST** be used to control available updates. Each patch **MUST** be assessed in terms of its effect on security. It **SHOULD** then be prioritised accordingly.

If apps have known vulnerabilities and no patches are available, appropriate countermeasures **MUST** be taken. If this is not possible, apps with known open vulnerabilities **MUST NOT** be used.

APP.1.4.A7 Secure Storage of Local App Data

If apps can access the organisation's internal documents, the local data storage of the app **MUST** be adequately secured. An access key **MUST** be stored in an encrypted form.

It **MUST** be ensured that confidential data is not cached by the operating system at other locations.

APP.1.4.A8 Preventing Data Leaks

To prevent unintended instances of apps sending confidential data or this data being used to create user profiles, app communication **MUST** be appropriately restricted. To this end, communication **SHOULD** be analysed as part of the testing and approval procedure. Checks **SHOULD** also be carried out to determine whether an app is writing unwanted log or auxiliary files that may contain confidential information.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module APP.1.4 *Mobile Applications (Apps)*. They **SHOULD** be implemented as a matter of principle.

APP.1.4.A9 Secure Connection to Back-end Systems [Process Owner]

The connection between app and back-end systems **SHOULD** be secured by cryptographic measures. In this regard, it **MUST** be checked whether the procedures offered by the operating system are sufficiently secure for the app, or whether in-house methods have to be implemented at the application level.

If an app accesses back-end systems, it **MUST** have its own service account.

APP.1.4.A10 Secure Authentication of Apps

Before an app can access an organisation's IT systems, it **SHOULD** authenticate itself through the back-end system. Appropriate and secure authentication mechanisms **MUST** be used for this. The app **MUST** transfer the authentication parameters (e.g. user name, password, certificate) using a secure protocol. If an employee loses a mobile device, it **SHOULD** be ensured that no unauthorised person can access the apps on it or use them as a means of accessing the organisation's information.

APP.1.4.A11 Central Management of Apps

An MDM solution **SHOULD** be established. Check mechanisms and whitelists **SHOULD** ensure that only tested and approved apps can be used.

APP.1.4.A12 Uninstalling Apps Securely

When apps are uninstalled, all the files generated by the app SHOULD also be deleted. This SHOULD also delete data temporarily stored by the operating system in relation to the app, such as caches. In addition, data stored on external systems (such as those operated by the app provider) SHOULD also be deleted.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.1.4 *Mobile Applications (Apps)* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.1.4.A13 Developing Fallback Solutions for Apps [Process Owner] (A)

An alternative solution SHOULD be available for all business processes mapped with apps in the event of disruption or other impediments. The maximum tolerable downtime of an app SHOULD be considered in advance, along with how the affected business processes can be mapped elsewhere – for example, through a central web portal.

APP.1.4.A14 Support for Additional Authentication Features for Apps (CI)

A second factor SHOULD be used for authentication in apps. Here, it SHOULD be ensured that any required sensors or interfaces are present in all devices used. In addition, biometric procedures SHOULD take into account how resistant authentication is to possible forgery attempts.

APP.1.4.A15 Performing Penetration Tests for Apps (CIA)

Before an app is approved for use, a penetration test SHOULD be performed. All communication interfaces to back-end systems, as well as the local storage of data, SHOULD be examined for possible vulnerabilities. The penetration tests SHOULD be repeated regularly and when major changes are made to the app.

Additional Information

For more information about threats and security measures for module APP.1.4 *Mobile Applications (Apps)*, see the following publications, among others:

[BKAPP]	Guide "Apps & Mobile Services – Tipps für Unternehmen": Empfehlung des BITKOM: „Apps und Mobile Services – Tipps für Unternehmen“ (2. Auflage, 2014), https://www.bitkom.org/Publikationen/2014/Leitfaden/Apps-und-Mobile-Services-Tipps-fuer-Unternehmen/140121-Apps-und-Mobile-Services-2014.pdf , last accessed on 07.09.2018
[BSIAPP]	BSI publication: "Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen" (2006), https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Mobile_Endgeraete.pdf , last accessed on 07.09.2018
[ISFAPP]	ISF: "Securing Mobile Apps – Embracing mobile, balancing control", 2018

[NIST800163]	NIST Special Publication 800-163: Vetting the Security of Mobile Applications, 2015, https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-163.pdf , last accessed on 07.09.2018
--------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module *APP.1.4 Mobile Applications (Apps)*:

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.42 Social Engineering

Elementary Threats Requirements	G 0.9	G 0.1 4	G 0.1 5	G 0.1 6	G 0.1 7	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 1	G 0.2 3	G 0.2 5	G 0.2 6	G 0.2 8	G 0.2 9	G 0.3 2	G 0.3 6	G 0.3 8	G 0.3 9	G 0.4 2
APP.1.4.A1	X	X	X	X	X	X	X				X	X		X			X		
APP.1.4.A2		X	X	X	X	X	X			X				X					X
APP.1.4.A3		X				X	X	X	X	X				X	X			X	
APP.1.4.A4						X						X	X	X	X			X	
APP.1.4.A5		X	X				X		X					X	X		X	X	X
APP.1.4.A6											X	X	X						
APP.1.4.A7		X		X	X		X												
APP.1.4.A8		X	X				X							X			X		
APP.1.4.A9	X	X	X				X			X									
APP.1.4.A10	X	X	X				X			X					X	X			
APP.1.4.A11						X								X					
APP.1.4.A12		X				X	X							X			X		
APP.1.4.A13	X					X					X	X							
APP.1.4.A14		X		X	X	X	X			X				X	X	X			
APP.1.4.A15									X	X	X	X	X						



APP.2.1: General Directory Service

Description

Introduction

A directory service provides information in a data network on any objects in a defined manner. Corresponding attributes can be stored with an object such as a user ID, first and last name of the user, their personnel number, and the name of their computer, for example. This data can then be used by any of the various applications. The directory service and its data are normally administered from a central location.

Some typical areas of application of directory services include:

- Administration of address books, e.g. for telephone numbers, email addresses, or certificates for electronic signatures
- Resource administration, e.g. for computers, printers, scanners, and other peripheral devices
- User administration, e.g. for the administration of user accounts and user authorisations
- Authentication, e.g. for logging in to operating systems or to applications

Directory services are optimised for read-only access, since data from the directory service is typically called. Write access such as creating, changing, or deleting entries are required less frequently.

Objective

The objective of this module is to securely operate general directory services, as well as to appropriately protect the information processed using the services.

Not in Scope

This module examines general security aspects of directory services regardless of which product is actually used. There are additional modules for product-specific security aspects in the IT-Grundschutz Compendium that should be applied to the corresponding directory service in addition to this module.

One example in this regard is Active Directory from Microsoft (see APP.2.2 *Active Directory*). Other directory services are based on the free OpenLDAP (see APP.2.3 *OpenLDAP*) used on many Unix-based systems and, for example also on Apple's MacOS. Modules on server systems

directory services usually are operated on can be found in the layer SYS.1 Servers of the IT-Grundschutz Compendium.

Threat Landscape

The following specific threats and vulnerabilities are of particular importance for the module APP.2.1 *General Directory Service*:

Lack of or Inadequate Planning of the Use of Directory Services

The security of directory services is based strongly on the security of the basic operating system, and especially on the file system security. Directory services can be installed and operated on a number of operating systems, and this may result in a wide variety of security settings to be performed. This variety increases the planning requirements and requires corresponding knowledge of the operating systems used as a basic operating system. If the resulting overall solution is very heterogeneous or complex, an inappropriately planned use of the directory service may cause vulnerabilities during actual operation. Since directory services furthermore usually allow a role-based administration of the directory database as well as the delegation of individual administration tasks, there is a threat that the system will be insecure or administered inefficiently if the administration tasks are planned incorrectly.

Lack of or Inadequate Planning of Partitioning and Replication in the Directory Service

Partitioning is the process of distributing the directory data of a directory service among separate areas (partitions). The replication of partitions of the directory service normally serves for load distribution purposes. Redundant data storage also improves the reliability and thereby increases the availability. For this reason, planning is critically important here as well, because it may be possible to subsequently change the partition and replication settings, but such changes may lead to problems under certain circumstances. Incorrect or inadequate planning of the processes of partitioning and replicating the directory service may lead to losses of data as well as to inconsistencies in the data stored, to poor availability of the directory service, to a lower overall system performance, and possibly even to failures.

Lack of or Inadequate Planning of Access to the Directory Service

The administration of system and data access rights is an extremely labour-intensive task in the context of a directory service, in which, in extreme cases, many manual work steps may need to be performed that may lead to errors and a lack of overview of the work performed. Inadequate planning regarding whether data and, if so, which data is allowed to be transmitted in plain text may lead to inconsistencies or contradictions with the internal security policies of the organisation. Incorrect planning of the security safeguards and technologies of the directory service to protect confidential data may also lead to incompatibilities or even to the failure of the encryption component, which may have immediate effects on confidentiality and integrity.

Incorrect Administration of System and Data Access Rights

Site access rights to an IT system and data access rights to stored data and IT applications may only be granted in the scope required for performing the corresponding tasks. This is also applicable to authorisations assigned to users and groups administered by a directory service. If these rights are administered improperly, this results in malfunctions if the required rights have not been assigned. On the other hand, there may be vulnerabilities if rights exceeding the necessary rights are assigned. If the access rights are assigned incorrectly or inconsistently in

the directory service, the security of the overall system will be significantly threatened as a result. Administration rights also are a very critical aspect. If these rights are assigned incorrectly, the entire administration concept could be in question and, under certain circumstances, the directory system administration may even become blocked.

Errors in the Configuration of Directory Service Access

In many deployment scenarios, additional applications such as Internet or Intranet applications must access the directory service. An incorrect configuration may result in access rights being assigned improperly or unauthorised access to the directory service being possible or in data for authentication purposes being transmitted in plain text and non-encrypted information can be spied on as a consequence.

Failure of Directory Services and Encryption

Technical failures due to hardware or software problems may lead to the failure of directory services or parts thereof. As a consequence, it may be temporarily impossible to access the data stored in the directory. In extreme cases, data may be lost. As a consequence, business processes and internal processes may be impaired. If functioning copies of the failed parts of the system are available, it will still be possible to gain access, but the performance may be limited under certain circumstances depending on the network topology selected.

Directory Services Compromised Due to Unauthorised Access

If an attacker successfully circumvented a necessary authentication procedure regarding the directory service, he/she will generally be able to access large amounts of data he/she is not authorised to access. As a consequence, the entire directory service may be compromised. Furthermore, unauthorised persons may access network resources or services due to extended authorisations. This may lead to an attacker circumventing all defence safeguards of the directory service. The affected system could then be impaired or could even be destroyed. The security of a directory service may also be threatened when anonymous users are allowed. Since their identity is not checked, anonymous users are initially able to send any query to the directory service and obtain at least some information on the structure and content of the directory service. If anonymous access is permitted, it will also be easier for attackers to conduct DoS attacks on the directory service, because they will have more access capabilities that are more difficult to control.

Requirements

The specific requirements of the module APP.2.1 *General Directory Service* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Data Protection Officer, Process Owner

Basic Requirements

The following requirements **MUST** be implemented for the module APP.2.1 *General Directory Service* as a matter of priority:

APP.2.1.A1 Creation of a security policy for directory services

A security policy for the directory service **MUST** be drawn up. This policy **SHOULD** be in agreement with the organisation's overall security concept.

APP.2.1.A2 Planning the use of directory services [Data Protection Officer, Process Owner]

The use of directory services **MUST** be planned carefully. In addition to specifying the use of the directory service, a model consisting of object classes and attribute types **MUST** be developed that meets the requirements arising from the intended use. When planning the directory service, Employee Representatives and the Data Protection Officer **MUST** be involved. An access control policy for the directory service that meets the corresponding needs **MUST** be designed. In general, the planned directory structure **SHOULD** be documented completely. Safeguards **SHOULD** be planned to prohibit anyone from collecting data from the directory service without authorisation.

APP.2.1.A3 Setting up access authorisations for directory services [Process Owner]

The administrative tasks for the administration of the directory service itself and for the actual data administration **MUST** be separated clearly. The administrative tasks **SHOULD** be delegated in such a way that there are no overlaps. All administrative task areas and authorisations **SHOULD** be documented sufficiently.

The data access rights of the user and administrator groups **MUST** be configured and implemented based on the security policy drawn up. In the event of possibly merging several directory service trees, the resulting effective rights **MUST** be verified.

APP.2.1.A4 Secure installation of directory services

An installation concept **MUST** be drawn up, according to which administration and access authorisations are already configured when installing the directory service.

APP.2.1.A5 Secure configuration and configuration changes of directory services

The directory service **MUST** be configured securely. In addition to the server, the clients (computers and programs) **MUST** also be involved in the secure configuration of a directory service infrastructure.

Administrative access to the directory service **MUST** be protected. When performing configuration changes of the networked IT systems, the users **SHOULD** be informed on maintenance work on time. Backups **SHOULD** be performed for all affected files and directories prior to any changes to the configuration.

APP.2.1.A6 Secure operation of directory services

The security of the directory service **MUST** be maintained constantly during operation. All policies, regulations, and processes referring to the operation of a directory service system **SHOULD** be documented. Access to all administration tools **MUST** be prohibited for normal users.

Standard Requirements

Together with the basic requirements, the following requirements correspond to the state-of-the-art technology for the APP.2.1 *General Directory Service* module. They SHOULD be implemented as a matter of principle.

APP.2.1.A7 Drawing up a security concept for the use of directory services

The directory service security concept SHOULD specify rules for all topics relevant to security for a directory service. The security policies developed from this SHOULD be documented in writing and the users of the directory service SHOULD be informed of the security policies to the required extent.

APP.2.1.A8 Planning of partitioning and replication in the directory service

The availability and the protection needs of the directory service SHOULD be taken into account while partitioning. The partitioning of the directory service SHOULD be documented in writing so that it can be reconstructed manually. In order to be able to perform the replication in a timely fashion, sufficient bandwidth SHOULD be made available.

APP.2.1.A9 Selection of suitable components for directory services [Process Owner]

Suitable components SHOULD be selected for the use of a directory service. A catalogue of criteria SHOULD be drawn up, on the basis of which the components for the directory service can be selected and acquired. The security requirements placed on the directory service SHOULD be formulated during the planning and design phases based on the purpose of the directory service.

APP.2.1.A10 Training on administration and operation of directory services

The administrators SHOULD be familiar with all security mechanisms and aspects of directory services covered by their scope of activities. They SHOULD be trained in this regard prior to configuration and regularly afterwards.

APP.2.1.A11 Setting up access to directory services

Access to the directory service SHOULD be configured according to the security policy. If the directory service is used as a server on the Internet, it SHOULD be protected accordingly by a security gateway. If anonymous users are to be granted more advanced access rights to individual sub-areas of the directory tree, a separate user account for the anonymous access, a so-called proxy user, SHOULD be created to this end. In addition, the data access rights for this proxy user SHOULD be assigned sufficiently restrictively. They SHOULD be removed completely if the account is not needed any more. In order to prevent the unnecessary disclosure of security-sensitive information, the search feature of the directory service SHOULD be limited as required by the purpose.

APP.2.1.A12 Monitoring directory services

In order to monitor directory services, a monitoring concept SHOULD be drawn up and implemented. Directory service-specific events and operating system-related events SHOULD be monitored, logged, and analysed.

APP.2.1.A13 Protection of communications with directory services

Data exchange between client and directory service server SHOULD be secured; this is particularly true for external connections. The data that may be accessed SHOULD be defined. In the

case of a service-oriented architecture (SOA), all requests sent to the registry SHOULD be checked for the validity of the user in order to protect service entries in a service registry.

APP.2.1.A14 Orderly withdrawal of a directory service from operation [Process Owner]

When withdrawing the directory service from operation, it SHOULD be ensured that continuously required rights and information are available in sufficient amounts, and that all other rights and information are deleted. Furthermore, the users SHOULD be informed of when a directory service is withdrawn from operation. When withdrawing individual partitions of a directory service from operation, it SHOULD be ensured that no other partitions will be affected by the withdrawal.

APP.2.1.A15 Migration of directory services

In the event of a scheduled migration of directory services, a migration concept SHOULD be drawn up beforehand. The schema changes performed on the directory service SHOULD be documented. Far-reaching authorisations used for performing the migration of the directory service SHOULD be withdrawn. The access rights for directory service objects on the systems that were updated to a new version or were obtained from other directory systems SHOULD be updated.

Requirement in Case of Increased Protection Needs

Generic suggestions for module APP.2.1 *General Directory Service* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.2.1.A16 Creation of a business continuity plan for the failure of a directory service (CIA)

Within the framework of contingency planning, a need-based business continuity plan SHOULD be drawn up for directory services. Business continuity plans SHOULD be present in case of the failure of important directory service systems. All contingency procedures for the overall system configuration of the directory service components SHOULD be documented.

Additional Information

For more information about threats and security safeguards for the APP.2.1 *General Directory Service* module, see the following publications, among others:

[ISFTM12]	The Standard of Good Practice for Information Security: Area TM 1.2 Security Event Logging, Information Security Forum (ISF), June 2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 05.09.2018
[TKOM1]	Privacy and Security Assessment process: Security Requirement: Proxy Server: Deutsche Telekom, October 2016, https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/sicherheit/privacy-and-security-assess-

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are important for the APP.2.1 *General Directory Service* module:

- G 0.11 Failure or Disruption of Service Providers
- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.33 Shortage of Personnel
- G 0.36 Identity Theft
- G 0.37 Repudiation of Actions
- G 0.38 Misuse of Personal Information
- G 0.39 Malware
- G 0.40 Denial of Service

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G0.1	G0.14	G0.15	G0.18	G0.19	G0.21	G0.22	G0.23	G0.25	G0.26	G0.27	G0.28	G0.29	G0.30	G0.31	G0.32	G0.33	G0.36	G0.37	G0.38	G0.39	G0.40	G0.42	G0.43	G0.44	G0.45	G0.46	
APP.2.1.A1				X				X							X	X												
APP.2.1.A2	X	X	X	X	X	X		X	X	X					X	X					X				X	X		
APP.2.1.A3	X	X	X	X	X	X	X	X							X	X	X	X	X						X	X	X	
APP.2.1.A4								X				X																
APP.2.1.A5	X			X					X	X					X	X					X							
APP.2.1.A6	X	X	X		X	X	X	X	X	X					X	X	X	X	X							X	X	
APP.2.1.A7				X								X																
APP.2.1.A8	X			X					X	X																	X	
APP.2.1.A9				X								X																
APP.2.1.A10	X			X	X			X	X	X	X	X	X	X	X	X	X	X	X	X			X		X	X	X	
APP.2.1.A11				X					X					X	X						X					X	X	
APP.2.1.A12				X				X	X	X	X				X	X	X		X		X	X	X					
APP.2.1.A13		X	X					X							X	X		X	X						X	X		

APP.2.1 .A14			X				X										X			X	
APP.2.1 .A15			X				X				X	X						X			X
APP.2.1 .A16	X		X				X														



APP.2.2: Active Directory

Description

Introduction

Active Directory Services (often abbreviated as AD or ADS) is a directory service developed by Microsoft that was introduced for the first time with the Windows 2000 Server operating system. Based on the Active Directory functions available in the Microsoft Windows 2000 Server operating system, additional key functions were added to the Active Directory service in every release of the Windows Server family of operating systems.

Active Directory is mainly used in IT networks that run primarily on Microsoft components. Active Directory stores information on objects within an IT network, e.g. information on users or computers, and makes it easier for users and administrators to provide, organise, use and monitor this information. Since Active Directory is an object-based directory service, it allows the administration of objects and their mutual relationships, which is what forms the actual network environment. Active Directory provides central control and monitoring capabilities for a given network. This type of directory service is especially useful in networks where the number of clients used in the network makes local administration difficult, for example. Without a directory service, it is impossible to guarantee the reliability of the settings to be implemented locally – the specifications of security policies, for example – because it would require too much personnel. Administration tasks in the network such as changing passwords, creating accounts, and specifying access rights can be performed more efficiently through the use of a directory service.

Objective

This module is designed to help secure Active Directory in normal operations at organisations (public authorities or companies) that use ADS to administer their infrastructure of Windows systems (client and server).

Not in Scope

This module examines the threats and safeguards which apply specifically to Active Directory. General security recommendations for directory services can be found in module APP.2.1 *General Directory Service*. The general safeguards described therein are explained in detail and complemented by this module. This module does not repeat the requirements regarding the process of securing the operating systems of servers and clients used to operate and administer AD (e.g. SYS.1.2.2 *Windows Server 2012* or SYS.2.2.3 *Windows 10 Clients*) and the underlying network infrastructure. Processes such as backups and patch management are also only addressed to the extent that particularities must be considered in the field of AD.

Threat Landscape

For module APP.2.2 *Active Directory*, the following specific threats and vulnerabilities are of particular importance:

Poor Planning of Security Limits

An AD instance generates a forest as a container at the highest level for all domains of the instance. A forest may include one or more domain container objects characterised by a common logical structure, a global catalogue, a scheme, and automatic transitive trust relationships. The forest – not a single tree – is thus the default security limit within which information is forwarded in AD. If these limits are not planned in a conscious and structured manner, information may leak out unintentionally and the security concept of the organisation may fail. As a consequence, it may be necessary to establish additional forests if different security requirements apply to certain parts of the infrastructure. However, this makes configuration and administration more complex.

Excessive or Overly Lax Trust Relationships

If the trust relationships between forests and domains are not evaluated regularly as to whether they are still needed and justified, whether they are of the proper type (in particular, whether a bilateral trust relationship is actually necessary), and whether the security controls are sufficient to ensure them, this may result in problems regarding authorisations and in information leaks. In particular, if the SID filtration (Security Identifier) that is active by default is disabled, complex vulnerabilities may occur that are difficult to understand. The same holds true if an organisation chooses not to implement selective authentication for trust relationships between forests.

Lack of Security Features Due to Older Operating Systems and the Domain Functional Level

Every new generation of the Windows Server operating system includes additional security features and extensions, including for AD. Furthermore, the default settings are made more secure with every new release. Some of them can be used once the new system has been installed, and others only after the domain/forest functional level has been increased. Along with obsolete domain functional levels, the use of older operating systems as (primary) domain controllers thus prevents the use of contemporary security features and increases the risk of insecure default settings. An insecurely configured domain endangers the information processed therein and makes it easier for third parties to carry out attacks.

Operation of Additional Roles and Services on Domain Controllers

Every additional service operated on a domain controller – except for AD itself, as well as a few auxiliary services absolutely required for AD, e.g. DNS – increases the number of potential attacks on these central infrastructure components due to possible additional vulnerabilities and improper configurations. These may be misused inadvertently or wilfully in order to copy or change information without authorisation, for example.

Misuse of the Group of Domain Administrators

AD itself should only be overseen by a very small number of administrators. In many cases, however, the number of accounts configured as DAs (domain administrators) is far greater than the number required. These accounts have full administrative rights on all domain controllers, workstations, group policies, etc. If attackers succeed in capturing one of these ac-

counts, they will have an unnecessarily large amount of freedom within the system. Frequently, the group of DAs includes service accounts and other groups not directly associated with the administration of AD itself.

Inappropriate Monitoring and Documentation of Delegated Rights

If the formation of company-specific groups and the process of delegating rights to them are not planned and implemented in a systematic manner, the delegation may get out of hand and grant much more access than intended, which may be misused by third parties. If the groups and their access rights are not audited on a regular basis, these rights will be at risk of escalating over the course of time. The use of default groups and the delegation of their rights to proprietary groups (e.g. by delegating "Account Operators" to helpdesk employees) also usually lead to more rights being granted than are actually required.

Insecure Authentication

So-called "legacy" (i.e. obsolete) authentication mechanisms in the field of AD, such as LM (LAN manager) and NTLM (NT LAN manager) v1, are considered insecure today and may be easily circumvented by attackers under certain conditions. As a consequence, an attacker may obtain or misuse rights without knowing, guessing, or otherwise cracking user passwords, and may thus compromise the domain or parts thereof.

AD Administrators Logging into Systems with Low Trust Levels

It must be assumed that malicious code will penetrate different systems, such as normal workstations or servers. An attacker who gains access by such means will be looking for additional credentials to misuse. If privileged accounts are able to log into all possible IT systems, the attacker will have myriad opportunities to obtain credentials and additional authorisations, particularly if the credentials are cached there.

Lack of Monitoring of Membership in Privileged Groups

In the majority of organisations, the number of accounts with administrative rights grows continuously and is rarely pared down (if it is at all). This violates the least privilege principle and results in more and more opportunities for attackers to obtain and misuse additional authorisations.

Overly Powerful or Insufficiently Secure Service Accounts

Application software providers sometimes grant DA rights to service accounts by default in order to facilitate the testing and deployment of their products even though significantly fewer rights would be necessary for operations. Additional rights for service accounts may be misused by attackers in order to access further areas of a domain. Since the credentials of a service that is executed in the context of a service account are stored in the protected memory of the LSASS, an attacker may extract them there. A single insufficiently secured service account may thus result in the entire domain being compromised.

This is particularly applicable if the service account is secured using a weak password. This is because an attacker may, when Kerberos authentication is in use, easily request a TGS (Ticket Granting Service) ticket in which the password of the service account is processed and crack the latter through brute force.

Use of the Same Local Administrator Password on Multiple Systems

Local accounts may log into a system even if the system is not connected to the domain. If the same credentials are used on several systems, the administrator may also log into the other systems. This increases the risk of an attacker finding domain credentials with higher rights on one of the systems and misusing these in order to compromise the domain.

Lack of Deletion of Accounts No Longer in Use from AD

Attackers may prefer trying to use accounts that are no longer used, but still exist in AD for attacks because any misuse may remain unnoticed for an extended period of time due to a lack of ownership.

Requirements

The specific requirements of module APP.2.2 *Active Directory* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Process Owner

Basic Requirements

For module APP.2.2 *Active Directory*, the following requirements **MUST** be implemented as a matter of priority:

APP.2.2.A1 Planning Active Directory [Process Owner]

The domain functional level selected **MUST** be appropriate and as high as possible. The justification **SHOULD** be documented appropriately. An Active Directory access control policy that meets the requirements at hand **MUST** be developed. Administrative delegations **MUST** be assigned restrictive authorisations that meet the requirements at hand. The planned Active Directory structure, including possible scheme changes, **SHOULD** be documented in a comprehensible manner.

APP.2.2.A2 Planning of Active Directory Administration [Process Owner]

A role-based access control policy **MUST** be drawn up. All administrative task areas and authorisations **SHOULD** be documented appropriately.

In large domains, the administrative users **MUST** be divided in terms of the service and data administration pertaining to Active Directory. Here, the administrative tasks **MUST** also be distributed in Active Directory according to a delegation model so that there is no overlap.

APP.2.2.A3 Planning of Group Policy in Windows

There **MUST** be a concept for configuring group policies. Multiple overlaps **MUST** be avoided whenever possible in the group policy concept. It **MUST** be possible to recognise the exceptions to the group policy concept in the documentation. All group policy objects **MUST** be protected by restrictive access rights. Secure specifications **MUST** be defined for the parameters in all group policy objects.

APP.2.2.A4 Training on Active Directory Administration

The administrators **MUST** be familiar with all the security mechanisms and aspects of Active Directory that pertain to their scope of activities. They **SHOULD** be trained to work with Active Directory prior to its configuration, and then at regular intervals.

APP.2.2.A5 Hardening Active Directory

Built-in accounts **MUST** be assigned complex passwords and only serve as emergency accounts. Privileged accounts **MUST** be members of the protected users group. Managed service accounts (for groups) **MUST** be used for service accounts.

All domain controllers **MUST** be assigned restrictive access rights at the operating system level. The Active Directory restore mode **MUST** be protected by an appropriate password. Work in this mode **SHOULD** only be performed in compliance with the two-person principle.

An image of the domain controller **SHOULD** be created at regular intervals. The authorisations for the “Everyone” group **MUST** be restricted. The domain controller **MUST** be protected against unauthorised restarts.

The policies for domains and domain controllers **MUST** include secure settings for passwords, account lockout, Kerberos authentication, user rights and monitoring. A sufficient size **MUST** be set for the security log of the domain controller. If external trust relationships exist with other domains, users' authorisation data **MUST** be filtered and anonymised.

APP.2.2.A6 Maintaining the Operational Continuity of Active Directory

All trust relationships in AD **MUST** be evaluated at regular intervals.

The service administrators on the domain controller **MAY** only possess the required rights. These rights **MUST** be evaluated at regular intervals. The domain administrators group **MUST** be empty or as small as possible. Accounts that are no longer used **MUST** be disabled in AD. They **SHOULD** be deleted after a reasonable retention period has expired.

All necessary parameters of Active Directory **SHOULD** be kept up to date and documented comprehensibly as basic information.

APP.2.2.A7 Implementation of Secure Administration Methods for Active Directory [Process Owner]

Administrator accounts **MAY NOT** be used for normal day-to-day work. Server administrator accounts **MAY NOT** be used on workstations. Domain administrator accounts **MAY NOT** be used on workstations or servers.

It **MUST** be possible to clearly trace every account to an employee.

The number of service administrators and data administrators for Active Directory MUST be limited to the required minimum of trustworthy persons. Their accounts MUST be protected appropriately.

The standard “Administrator” account SHOULD be renamed and an unprivileged account named “Administrator” SHOULD be created. Day-to-day, non-administrative tasks MUST be performed using unprivileged user accounts.

It MUST be ensured that the administration of service administrator accounts is only performed by members of the Service Administrator group. The “Account Operators” group SHOULD be empty.

Administrators SHOULD only be assigned to the “Scheme Administrators” group temporarily for the time required to change the scheme. For the groups “Organisational Administrators” and “Domain Administrators”, the two-person principle SHOULD be established for administration of the root domain.

The workstations used for administration of Active Directory MUST be adequately protected. If the domain controllers are subject to remote administration, the data transmitted MUST be appropriately encrypted.

It MUST be ensured that the “Administrators” and “Domain Administrators” groups are owners of the domain root object of the domain in question.

The use of domain-local groups for controlling the read privileges of object attributes SHOULD be avoided.

The recycle bin of AD SHOULD be enabled.

In large organisations, an enterprise identity management solution SHOULD be used in order to ensure that the rights of all users comply with defined specifications.

Standard Requirements

For module APP.2.2 *Active Directory*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

APP.2.2.A8 Configuration of Secure Channel in Windows

Secure Channel SHOULD be configured in Windows according to the security requirements and the local conditions at hand. All relevant group policy parameters SHOULD be taken into account in the process.

APP.2.2.A9 Authentication Protection When Using Active Directory

The Kerberos authentication protocol SHOULD be used consistently in the Active Directory environment. If NTLMv2 is used temporarily due to compatibility reasons, the migration to Kerberos SHOULD be planned and scheduled. LM authentication SHOULD be disabled. SMB data traffic SHOULD be signed. Anonymous access to domain controllers SHOULD be prevented.

APP.2.2.A10 Secure Use of DNS for Active Directory

Integrated DNS zones or secure dynamic updating of DNS data SHOULD be used in order to prevent DNS client requests from unauthorised systems. Access to the configuration data of the DNS server SHOULD only be permitted from administrative accounts. The DNS cache on the DNS servers SHOULD be protected against unauthorised changes. Access to the DNS service of the domain controllers SHOULD be restricted to the required extent. Network activities related to DNS requests SHOULD be monitored. Access to the DNS data in Active Directory SHOULD be restricted to administrators using ACLs.

Secondary DNS zones SHOULD be avoided. At minimum, the zone file SHOULD be protected against unauthorised access.

If IPsec is being used in order to protect DNS communications, sufficient data throughput SHOULD be ensured within the network.

APP.2.2.A11 Monitoring the Active Directory Infrastructure

The Active Directory infrastructure SHOULD be monitored and logged based on the system-internal events. The security monitoring results regarding Active Directory SHOULD be evaluated at regular intervals. The availability and the system resources of the domain controllers SHOULD be monitored. Changes at the domain level and in the overall structure of Active Directory SHOULD be monitored, logged and evaluated.

APP.2.2.A12 Backups for Domain Controllers

There SHOULD be a backup and recovery policy for domain controllers. The backup software used SHOULD be explicitly approved by the provider for use in backing up the data of domain controllers. A separate backup account with service administrator rights SHOULD be set up for the domain controllers. The number of members of the “Backup Operators” group SHOULD be restricted to the required minimum. Access to the AdminSDHolder object SHOULD be placed under special protection in order to protect the authorisations.

The data of the domain controllers SHOULD be backed up at regular intervals. Here, a method that avoids legacy objects whenever possible SHOULD be used.

The backup media SHOULD be stored at a suitable location. Regular checks SHOULD be carried out to ensure that the correct backup procedure is being followed and the process of restoring backups of domain controllers works as intended.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.2.2 *Active Directory* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.2.2.A13 Two-Factor Authentication (CIA)

Privileged accounts in the field of AD SHOULD be protected with the help of two-factor authentication.

APP.2.2.A14 Dedicated Privileged Administration Systems (CIA)

The administration of Active Directory SHOULD be limited to dedicated administration systems. These SHOULD be subject to particularly strong hardening based on limited tasks.

APP.2.2.A15 Separation of Administration and Production Environments (CIA)

Particularly critical systems such as domain controllers and domain administration systems SHOULD be separated in a separate forest with a unilateral trust towards the production forest.

Additional Information

For more information about threats and security safeguards for module APP.2.2 *Active Directory*, see the following publications, among others:

[ADRL]	AD Reading Library : (Active Directory Security), with further AD Security Blog literature, https://adsecurity.org/page_id=41 , last accessed on 24.08.2018
[ESAE]	Enhanced Security Administrative Environment: Microsoft TechNet https://docs.microsoft.com/de-de/windows-server/identity/securing-privileged-access/securing-privileged-access , last accessed on 09.08.2018
[PAW]	Privileged Access Workstations: Microsoft TechNet, April 2016, http://download.microsoft.com/download/9/3/9/9392A4D2-D530-4344-8447-4A7CF1C01AEE/Privileged%20Access%20Workstation_Datasheet.pdf , last accessed on 09.08.2018
[TN283324]	Entry point for Active Directory for Windows Server 2012 (R2): Microsoft TechNet, https://technet.microsoft.com/en-us/library/dn283324.asp , last accessed on 09.08.2018
[TN378801]	Entry point for Active Directory for Windows Server 2008 R2: Microsoft TechNet, May 2009, https://technet.microsoft.com/en-us/library/dd378801.aspx , last accessed on 09.08.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.2.2 *Active Directory*:

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.40 Denial of Service

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G0.1	G0.14	G0.15	G0.18	G0.19	G0.21	G0.22	G0.23	G0.25	G0.26	G0.27	G0.28	G0.29	G0.30	G0.31	G0.32	G0.33	G0.36	G0.37	G0.38	G0.39	G0.40	G0.42	G0.43	G0.44	G0.45	G0.46
APP.2.2.A1	X	X	X	X	X	X		X		X	X					X		X				X			X	X	
APP.2.2.A2	X	X	X	X	X	X	X	X							X	X	X		X		X				X		X
APP.2.2.A3		X	X	X	X	X		X								X		X							X		X
APP.2.2.A4	X			X	X			X		X	X	X	X	X	X	X	X			X			X		X	X	X
APP.2.2.A5		X	X		X	X	X	X				X	X	X		X		X	X	X	X	X		X	X	X	X
APP.2.2.A6		X	X		X	X	X	X				X	X	X		X		X	X	X	X	X		X	X	X	X
APP.2.2.A7	X	X	X	X	X	X	X	X						X	X	X		X		X					X		X
APP.2.2.A8		X	X		X	X	X	X						X				X							X		X
APP.2.2.A9		X	X		X	X	X	X						X				X							X		X
APP.2.2.A10								X						X									X	X	X	X	X
APP.2.2.A11				X				X	X	X	X			X	X	X		X		X	X	X	X				
APP.2.2.A12									X									X		X	X				X		
APP.2.2.A13					X	X	X	X						X				X									

APP.2.2 .A14	X	X		X	X	X	X						X	X	X			X								
APP.2.2 .A15	X	X		X	X	X	X						X	X	X			X								



APP.2.3: OpenLDAP

Description

Introduction

OpenLDAP is a freely available directory service that provides information in a data network using any objects, such as users or IT systems, in a defined manner. The information can include simple attributes – the names or numbers of objects, for example, but also complex formats such as photos or certificates – for electronic signatures. The typical fields of application include address books and user administration systems.

OpenLDAP is a reference implementation for a server service within the framework of the Lightweight Directory Access Protocol (LDAP). Since it is open-source software, OpenLDAP can be installed on a variety of operating systems and is one of the most widely used directory services. Overlays are a special feature of OpenLDAP. Overlays add numerous functions to OpenLDAP and are also used for basic functions such as logging, replication and maintaining integrity.

Objective

The objective of this module is to facilitate the secure operation of directory services based on OpenLDAP and appropriate protection of the information processed using these services.

Not in Scope

This module examines the threats and requirements that apply specifically to OpenLDAP. It does so based on Version 2.4 of OpenLDAP. The general security recommendations for directory services found in module APP.2.1 *General Directory Service* must also be taken into account. The present module explains the requirements described there in detail and provides further supplementary information.

Threat Landscape

For module APP.2.3 *OpenLDAP*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Inadequate Planning of OpenLDAP

OpenLDAP can be used with many other applications that can access the directory service's information and usually change it, as well. If the use of OpenLDAP is insufficiently planned or not planned at all, the following problems may occur:

- If the back ends and the associated directives and parameters are selected incorrectly, they will unintentionally influence the functions that OpenLDAP can offer. If, for example, the back-ldif back end is used for data storage to avoid the installation of an additional database, only rudimentary functions of the directory service will be available. This will make it impossible to appropriately manage a large number of users or other objects.
- If the use of overlays is poorly planned, unnecessary operations will be performed or other functions impaired in OpenLDAP. For example, access to the directory service can be incorrectly logged (or not logged at all) if the debug function of the slapd server itself and the auditlog and accesslog overlays are insufficiently planned.
- OpenLDAP can run in an unsuitable system environment. If a distributed file system such as NFS (Network File System) is used to store the OpenLDAP data, OpenLDAP or BerkeleyDB file functions will not be available. An example of this is the locking function used by many databases, which allows the user to lock the directory service database if another user wants to access the database in parallel.
- Incompatible versions of one or more applications could access the databases used by OpenLDAP. For example, the LDAPv3 protocol specifications are not met by OpenLDAP without additional extensions. In addition, there can also be connection problems with the applications if the wrong version of one or more programs are used that are not compatible with OpenLDAP.

Errors in the Assignment of Data Access Rights

OpenLDAP is closely connected to the operating system on which it is used. Some critical data for system users and resources is also managed from here, which makes the correct allocation of data access rights in OpenLDAP particularly important. If, for example, administration rights are assigned incorrectly during the implementation of a role-based administration concept or the delegation of individual administration tasks, the entire administration concept could be bypassed and the administration of OpenLDAP may even be disrupted.

Improper Configuration of OpenLDAP

OpenLDAP has numerous functions that enable the directory service to be used by many users with different needs. Incorrect configuration of these numerous functions can lead to unauthorised access to the directory service. If, for example, the standard configuration is not sufficiently checked and adapted, the authentication information can be transmitted in plain text. Malicious users could tap into unencrypted transmissions of this and other information and misuse it for further attacks.

Inadequate Separation of Offline and Online Access to OpenLDAP

The data managed by OpenLDAP (objects in the directory service and the configuration settings) can be accessed in various ways. Here, the offline and online access options fulfil partially or completely identical functions. For online access, the LDAP protocol is used to access the data; for offline access, the BerkeleyDB database files are accessed directly. If the access options are mixed or the respective method of operation for offline or online access is not understood, numerous error situations might occur. For example, when backing up and restoring data using the BerkeleyDB tools, the application-specific timestamps are not correctly restored; this means that the recovered database will be inconsistent with OpenLDAP and no longer usable.

Failure of Directory Services and Encryption

OpenLDAP can fail completely or partially due to hardware or software problems. As a consequence, it may be temporarily impossible to access the data stored in the directory. In extreme cases, data can be lost, hindering business processes and internal processes. A technical defect in a central cryptographic module can also significantly affect the functionality of a directory service. Encrypted data can then not be decrypted as long as the required cryptographic module is not available. This can result in availability problems for the directory service, for example, or other applications that process the decrypted data. If functioning copies of the failed parts of the system are available, these can still be accessed, but the performance may be limited under certain circumstances.

Directory Services Compromised Due to Unauthorised Access

If attackers can successfully circumvent a necessary authentication procedure for the directory service, they will be able to access large amounts of data without authorisation. As a consequence, the entire directory service may be compromised. Furthermore, unauthorised persons may access network resources or services due to extended authorisations. The security of OpenLDAP may also be threatened when anonymous users are allowed to log in. Since their identity is not checked, they are initially able to send any query to the directory service and obtain at least some information on its structure and content. If anonymous access is permitted, it will also be easier for attackers to conduct DoS attacks on OpenLDAP because they will have more access capabilities that are difficult to control.

Requirements

The specific requirements of the module APP.2.3 *OpenLDAP* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Data Protection Officer, IT Operation Department, Head of IT

Basic Requirements

For module APP.2.3 *OpenLDAP*, the following requirements **MUST** be implemented as a matter of priority:

APP.2.3.A1 Planning and Selecting Back Ends and Overlays for OpenLDAP [IT Operation Department, Head of IT]

The use of OpenLDAP in an organisation **MUST** be carefully planned. If OpenLDAP is to be used together with other applications, the planning, configuration and installation of applications and OpenLDAP **MUST** be harmonised. The version of the database used for data storage **MUST** be checked to ensure it is compatible. Back ends and overlays for OpenLDAP **MUST** be selected restrictively. It **MUST** be ensured that the OpenLDAP overlays are used in the correct

order for this purpose. When planning OpenLDAP, the client applications to be selected and supported MUST be considered.

APP.2.3.A2 Secure Installation of OpenLDAP

Checks MUST be carried out to determine whether all the applications that are to access OpenLDAP are compatible with the version to be installed. The versions of the OpenLDAP installation packages MUST be carefully selected and their integrity verified. All installation steps and the origin of the OpenLDAP installation packages SHOULD be documented.

APP.2.3.A3 Secure Configuration of OpenLDAP

Secure configuration of OpenLDAP requires a correctly configured slapd server. The client applications used MUST also be securely configured. When configuring OpenLDAP, the permissions MUST be set correctly in the operating system. The default values of all relevant OpenLDAP configuration directives MUST be checked and adapted if necessary. The back ends and overlays of OpenLDAP MUST be included in the configuration. Appropriate time and size restrictions MUST be set for searching within OpenLDAP. The configuration on the slapd server MUST be checked after each change.

APP.2.3.A4 Configuration of the Database Used by OpenLDAP

The access rights for newly created database files MUST be limited to the user ID in whose context the slapd server is run. The standard settings of the BerkeleyDB used by OpenLDAP MUST be adapted.

APP.2.3.A5 Secure Assignment of Access Rights to OpenLDAP

An access control policy MUST be defined using the method described in module APP.2.1 *General Directory Service*. The regulations specified in this concept MUST be implemented technically in OpenLDAP. The global and database-specific access control lists maintained in OpenLDAP MUST be factored in correctly when using OpenLDAP. Database directives MUST take precedence over global directives.

APP.2.3.A6 Secure Authentication for OpenLDAP

If the directory service is to distinguish between different users, they MUST authenticate themselves appropriately. The authentication between the slapd server and the communication partners MUST be encrypted. ONLY the hash values of passwords may be stored on the clients and servers. A suitable hashing algorithm MUST be used.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module APP.2.3 *OpenLDAP*. They SHOULD be implemented as a matter of principle.

APP.2.3.A7 OpenLDAP Training for Administrators

All administrators SHOULD be trained in OpenLDAP and the associated security topics.

APP.2.3.A8 Restrictions on Attributes in OpenLDAP

The attributes in OpenLDAP SHOULD be restricted using overlays. OpenLDAP SHOULD be modified so that values in the directory service only correspond to a specific regular expression. In addition, it SHOULD be ensured with the help of overlays that selected values only exist once in the directory tree. Such restrictions SHOULD only be applied to user data.

APP.2.3.A9 Partitioning and Replication in OpenLDAP

OpenLDAP SHOULD be partitioned into subtrees on different servers. In this case, changes to the data SHOULD be exchanged between the servers by replication. The replication mode SHOULD be selected depending on the network connections and availability requirements.

APP.2.3.A10 Secure Updating of OpenLDAP

The OpenLDAP software SHOULD be updated as soon as possible to new releases that contain security changes or fix vulnerabilities. Particular attention SHOULD be paid to whether the changes relate to the back ends or overlays used, or to software dependencies. If administrators use their own scripts, such scripts SHOULD be checked to see if they work with the updated version of OpenLDAP without any problems. The configuration and access rights SHOULD be carefully checked after an update.

APP.2.3.A11 Restriction of the OpenLDAP Runtime Environment

The slapd server SHOULD be restricted to a runtime directory. This directory SHOULD contain all configuration files and databases.

APP.2.3.A12 Logging and Monitoring of OpenLDAP [Data Protection Officer]

All relevant activities in OpenLDAP SHOULD be logged and monitored. The live operation of the slapd server SHOULD be monitored with suitable tools. The log data SHOULD be evaluated regularly in compliance with the organisation's internal requirements. OpenLDAP SHOULD be monitored together with the server running OpenLDAP.

APP.2.3.A13 Backup from OpenLDAP

The OpenLDAP server data, including its directory service objects and configuration settings, SHOULD be backed up regularly. In addition, all the OpenLDAP server partitions SHOULD be included in data backups. A suitable tool SHOULD always be used for recovering data.

Requirements in Case of Increased Protection Needs

For module APP.2.3 *OpenLDAP* there are no Requirements in Case of Increased Protection Needs.

Additional Information

For more information about threats and security measures for module APP.2.3 *OpenLDAP*, see the following publications, among others:

[ISFTM12]	The Standard of Good Practice for Information Security: Area TM 1.2 Security Event Logging, Information Security Forum (ISF), June 2018
[MASTERAR]	Konzeption und Erstellung eines IT-Grundschutz-Bausteins für den Verzeichnisdienst OpenLDAP: Master Thesis, Ruhr-Universität-Bochum, July 2010, https://www.b-si.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Extern/Diplomarbeiten/OpenLDAP_Steinkamp.pdf , last accessed on 18.07.2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on

	15.11.2017
[OpenLDAP]	OpenLDAP: community developed LDAP software: https://www.openldap.org/ , last accessed on 18.07.2018
[TKOM1]	Privacy and Security Assessment Process: proxy server security requirements: Deutsche Telekom, October 2016, https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/sicherheit/privacy-and-security-assessment-verfahren-342724 , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.2.3 *OpenLDAP*:

G 0.11 Failure or Disruption of Service Providers

G 0.15 Eavesdropping

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.38 Misuse of Personal Information

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

Elementary Threats Requirements	G 0.11	G 0.15	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.29	G 0.30	G 0.38	G 0.43	G 0.45
APP.2.3.A1		X		X	X		X				X	
APP.2.3.A2		X							X			
APP.2.3.A3		X						X	X			
APP.2.3.A4	X		X					X			X	X
APP.2.3.A5		X	X					X				
APP.2.3.A6		X						X				
APP.2.3.A7						X			X			
APP.2.3.A8												X
APP.2.3.A9		X				X					X	
APP.2.3.A10		X							X			
APP.2.3.A11		X					X			X		
APP.2.3.A12		X										
APP.2.3.A13		X									X	



APP.3.1: Web Applications

Description

Introduction

Web applications provide functions and dynamic content over the Internet protocol HTTP (Hypertext Transfer Protocol) or HTTPS (HTTP via SSL or TLS, which means they are protected by an encrypted connection). To accomplish this, documents and user interfaces (for example, input masks) are generated and delivered to corresponding client programs (web browsers). Web applications are usually developed on the basis of frameworks. These provide a basis for frequently recurring tasks (e.g. for security components).

As a general rule, several IT system components are required for operation of a web application. These usually include a web server to deliver data, an application server to operate the actual application and additional background systems connected as data sources by means of various interfaces (for example, database or directory service).

Web applications are used both in public IT networks and corporate networks (intranets) to provide data and applications. Depending on the purpose of the web applications, they are usually used by users who have to authenticate themselves in advance. For this reason, web applications must implement security mechanisms that ensure the protection of the data and prevent it from being misused. Some typical security components or mechanisms include authentication, authorisation, input validation, output encoding, session management, error handling and logging.

Objective

The objective of this module is to ensure the secure operation of web applications and protect the information they process.

Not in Scope

This module examines the threats and requirements applying specifically to web applications. Web applications provide functions and prepare dynamic content that is delivered by the web server (see also APP.3.2 *Web Servers*). Module APP.3.2 *Web Servers* also covers the editorial planning of websites and business continuity management, which is why these aspects are not discussed again in module APP.3.1 *Web Applications*. The security-relevant aspects of a service-oriented architecture (SOA) (see APP.3.7 *Service-Oriented Architectures*) are also not considered in this module.

Threat Landscape

For module APP.3.1 *Web Applications*, the following specific threats and vulnerabilities are of particular importance:

Deficiencies in the Development and Extension of Web Applications

If a web application is developed or extended with non-existent or inadequate specifications and standards, this can result in errors, loss of quality or incomplete functionality. In many cases, errors made in previous phases are only discovered at an advanced stage of development. To eliminate these errors after the fact, the source code of the web application often needs to be checked extensively and corrected again. This can result in a significant increase in development costs. In the case of fundamental architectural errors, the development of a completely new web application might even be required. Furthermore, if there are no specifications for the implementation of security mechanisms, the data to be processed may not be adequately protected.

Bypassing Authorisations in Web Applications

Attackers often try to access functions or data of web applications which are only available to a limited group of users. If authorisation is implemented improperly, in some circumstances an attacker could gain access to the authorisations of another user with more comprehensive rights and thereby access protected areas and data. This usually happens when an attacker deliberately manipulates input data.

Insufficient Input Validation and Output Encoding

If a web application processes unchecked input data which has been manipulated by an attacker, protection mechanisms may be bypassed. The output data of the web application is also transmitted either directly to the user's browser, the application making the request or downstream systems. If the data is not adequately encoded before output, it may contain malicious code which can then be interpreted or executed on the target systems.

Non-Existent or Insufficient Error Handling by Web Applications

If errors occur during operation of a web application, this can, for example, limit the availability of the web application or even make it unavailable. As a result, tasks may not be completed fully, temporarily cached states and data may be lost and security mechanisms may fail. Failure to handle errors correctly can impair both operations and the protection of functions and data.

Insufficient Logging of Security-Relevant Events

If security-related events are insufficiently logged by the web application, it may not be possible to trace them and eliminate their causes at a later point in time. Critical errors and attacks, such as unauthorised changes in the configuration of the web application, can thus remain undetected. Inadequate logging also makes it difficult to identify and fix vulnerabilities.

Disclosure of Security-Relevant Information in Web Applications

Websites and data generated and delivered by a web application can contain information on related background systems, e.g. information on IT components and versions of frameworks. This information can make it easier for an attacker to target the web application.

Misuse of a Web Application Due to Automated Use

If attackers use functions of a web application in an automated manner, they can perform numerous operations in a short time and thus efficiently carry out attacks on the web application that are based on repetition. Using a repeated login process, an attacker can, for example, attempt to determine valid combinations of user names and passwords (brute force) or generate lists of valid user names (enumeration). In addition, calling up resource-intensive functions repeatedly (e.g. complex database queries) can be misused for denial-of-service attacks at the application level.

Inadequate Session Management in Web Applications

An attacker who is able to determine the session ID of an authorised user due to inadequate session management may be able to access protected functions and resources of the web application. Session fixation attacks are one typical example: the attacker first acquires a session ID from the web application and then transmits this ID to a legitimate user (for example, via a link in an e-mail). If the user follows this link and logs into the web application with the session ID transmitted by the attacker, the attacker can then use the application with this known session ID. In this way, the attacker will be able to access the web application within the security context of the attacked user and use any protected functions.

Requirements

The specific requirements of module APP.3.1 *Web Applications* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Procurement Agent, Tester, Head of Development, Developer, Head of IT

Basic Requirements

For module APP.3.1 *Web Applications*, the following requirements **MUST** be implemented as a matter of priority:

APP.3.1.A1 Authentication for Web Applications [Developer]

To be able to access protected resources of a web application, users **MUST** authenticate themselves for the application. For this purpose, a suitable authentication method **MUST** be chosen and the selection process documented. If Basic-Auth is used, transport encryption **MUST** be used. The password files on the web server **MUST** be adequately protected.

A central authentication component which was implemented with as many established standard components as possible **MUST** be used. The component **MUST** force the users to use secure passwords in accordance with a password policy. If a web application stores authentication

data on a client, the user **MUST** explicitly consent ("opt-in") and be made aware of the risks the feature entails.

In order to ensure that a valid session (session ID) was not taken over by an attacker, the users **MUST** re-authenticate for critical functions. Limits on failed login attempts **MUST** also be defined in the web application. All the authentication processes the web application offers **MUST** have the same security level. Moreover, users **MUST** be informed immediately if their password has been reset.

APP.3.1.A2 Access Control for Web Applications [Developer]

An authorisation component **MUST** ensure that users can only perform actions for which they are authorised. Every attempt to access protected content and functions **MUST** be checked before being implemented.

All users **MUST** be assigned restrictive access rights in an orderly fashion. If employees are granted access rights for a web application or these rights change, the persons in charge **MUST** check and confirm this and document it in a comprehensible manner. The documentation of the access rights assigned **MUST** always be up to date. There **MUST** also be a controlled procedure for withdrawing access rights from users. If it is not possible to assign access rights, an additional security product **MUST** be used for this purpose.

The authorisation component **MUST** take into consideration all the resources managed by the web application. The users **MUST** be authorised on the server and centrally on a trustworthy IT system. If the access control system is defective, access **MUST** be denied. Access control **MUST** also be in place for URL calls and object references. User access to files **MUST** also be limited by restrictive file system authorisations, and a policy regarding the secure handling of temporary files **MUST** be in place.

APP.3.1.A3 Secure Session Management [Developer]

Session IDs **MUST** be protected adequately. They **MUST** be generated randomly (with adequate entropy). If the framework underlying the web application can generate session IDs, this function **MUST** be used. If session IDs are generated and managed by means of a framework, the framework **MUST** be configured in a secure manner. The session ID **MUST** also be protected adequately when it is transmitted and stored on the client.

A web application **MUST** provide the users with the option to expressly terminate an active session. After the user has logged in, any existing session ID **MUST** be replaced by a new one. Sessions **MUST** have a maximum timeout period. Inactive sessions **MUST** automatically expire after a specified period of time. After the session has become invalid, all session data (on both the server and the client) **MUST** become invalid and be deleted.

APP.3.1.A4 Controlled Integration of Data and Content in Web Applications [Developer]

It **MUST** be ensured that a web application only integrates designated data and content for delivery to the user. If a web application offers an upload function for files, this function **MUST** be restricted as much as possible. In this case, access and execution rights **MUST** also be set restrictively. Furthermore, it **MUST** be ensured that a user can save files only in the specified path. The storage location for uploads **MAY NOT** be influenced by the user.

The destinations of the redirection function of a web application **MUST** be restricted sufficiently so that users are only redirected to trustworthy websites. If a user leaves the trustworthy domain, they **MUST** be informed.

APP.3.1.A5 Logging Security-Relevant Events of Web Applications and Web Services [Developer]

A web application **MUST** log security-relevant events and their required characteristics in a traceable manner. Access to the logging data **MUST** be restricted to a few authorised persons. When the logging data is analysed, it **MUST** be ensured that malicious code in log entries will not be interpreted by the analysis program.

The legal requirements regarding logging and the handling of logging data **MUST** be observed.

APP.3.1.A6 Prompt Installation of Security-Relevant Patches and Updates

Administrators **MUST** regularly inform themselves about current vulnerabilities and promptly install security-relevant updates. Software updates and patches for web applications **MUST** only be obtained from trustworthy sources. They **MUST** be tested sufficiently before being rolled out. Before updates or patches are installed, it **MUST** always be ensured that the original state of the web application can be recovered. The current patch level **MUST** be documented.

APP.3.1.A7 Protection Against Unauthorised Automated Use of Web Applications [Developer]

Web applications **MUST** be protected against automated access by appropriate protection mechanisms. However, this **MUST** take into account the impact that the protection mechanisms will have on the ability of authorised users to use the application. If the web application contains RSS feeds or other functions explicitly intended for automated use, this **MUST** also be taken into account when configuring the protection mechanisms.

Standard Requirements

For module APP.3.1 *Web Applications*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

APP.3.1.A8 System Architecture of a Web Application

Security aspects **SHOULD** already be taken into account in the design phase of a web application. It **SHOULD** also be ensured that the architecture of the web application maps the exact business logic of the organisation and implements it correctly.

In the system architecture, provisions **SHOULD** be made to ensure that each server service will run on a separate IT system. Separate user accounts **SHOULD** also be used for the different server processes of the system components. Here, the rights of these service accounts **SHOULD** be restricted at the operating system level to the extent that access is only possible to the required resources and files of the operating system.

The network architecture **SHOULD** have several tiers (multi-tier architecture). At minimum, the security zones web tier, application tier and data tier **SHOULD** be taken into account in this respect. It **SHOULD NOT** be possible to access systems in the intranet from these zones.

The software architecture of the web application **SHOULD** be documented with all its components and dependencies. The documentation **SHOULD** already be updated and adapted during the course of the project to ensure that it can already be used during the development phase, and that the decisions taken are comprehensible. Components which are required for operation, but are not components of the web application **SHOULD** be marked and identified as such in the documentation. This documentation **SHOULD** also describe which components

implement which security mechanisms, how the web application is integrated into an existing infrastructure and which cryptographic functions and procedures are used.

APP.3.1.A9 Procurement, Development and Extension of Web Applications [Tester, Head of Development, Developer, Procurement Agent]

If products are procured for web applications, a requirements catalogue SHOULD be created. To be able to compare different products, an assessment scale SHOULD be developed.

If the actual web application or an extension thereof is developed in-house, an appropriate procedural model SHOULD be used. Prior to commissioning, all phases of the model SHOULD be completed. For development, programming guidelines which help to establish a uniform level of security SHOULD be specified.

When the security mechanisms of a web application are designed and developed, they SHOULD preferably take future standards and attack techniques into account. The development, test, and production environments SHOULD be separated during application development.

If the web application is developed by a service provider, it SHOULD be ensured that this service provider implements the necessary security requirements for development and the customer can access the source code at all times.

APP.3.1.A10 Testing and Approval of Web Applications [Head of IT]

Web applications or extensions that were either developed in-house or by a third party SHOULD be tested before they are incorporated into a production environment. The results of the tests SHOULD be documented. If the tests are successful, the web application SHOULD be formally approved. A troubleshooting procedure SHOULD also be established.

APP.3.1.A11 Secure Integration of Background Systems

Background systems to which web applications outsource functionalities and data SHOULD be protected adequately. The access to background systems SHOULD only be possible via defined interfaces and from defined systems. The data traffic between the users and the web application, applications and other services, and the corresponding background systems SHOULD be regulated by means of security gateways. When communicating across site and network boundaries, data traffic SHOULD also be authenticated and encrypted. The web application's attempts to access background systems SHOULD also be made with minimal rights.

When using an enterprise service bus (ESB), it MUST be ensured that all services must authenticate themselves with the ESB before they are granted access. A separate logical network segment SHOULD be available for the ESB. The ESB SHOULD only be accessed by connected applications and services. Any access to the ESB SHOULD be authenticated and encrypted for communications across location and network boundaries.

APP.3.1.A12 Secure Configuration of Web Applications [Developer]

A web application SHOULD be configured in such a way that its resources and functions can only be accessed using the secured communication paths specified for this purpose. Access to resources and functions that are not required SHOULD therefore be restricted. The following aspects SHOULD be taken into consideration when configuring web applications:

- deactivation of unnecessary HTTP methods

- character coding configuration
- definition of thresholds for access attempts
- web application administration

APP.3.1.A13 Restrictive Disclosure of Security-Related Information [Developer]

The websites and responses of web applications SHOULD not contain information which could make attackers aware of security mechanisms they can bypass. It SHOULD also be ensured that:

- Only neutral error messages are displayed.
- No security-relevant comments or product and version information is disclosed.
- There is only limited access to security-relevant documentation.
- Unneeded files are deleted regularly.
- External search engines register the web application appropriately.
- Absolute local path information is omitted.

The web application SHOULD NOT be administered from insecure networks. Administration access SHOULD be restricted to trusted separate network segments and IT systems. Configuration files of the web application SHOULD be saved outside the web root directories.

APP.3.1.A14 Protection of Confidential Data [Developer]

Confidential data of a web application SHOULD be protected by secure cryptographic algorithms. If such data is transmitted, secure, state-of-the-art transport encryption SHOULD be used. In the case of connection errors, the application SHOULD NOT switch from an encrypted channel to an unencrypted channel. The HTTP POST method SHOULD be used to transfer data from the client to the server.

The web application SHOULD also use directives to ensure that no sensitive data is cached on the client. Furthermore, no confidential form data SHOULD be shown as plain text in forms, and it also SHOULD NOT be saved by the browser. Web application access data SHOULD be protected against unauthorised access on the server with the help of cryptographic algorithms (salted hash). It SHOULD also not be possible to call files with source texts of the web application.

APP.3.1.A15 Verification of Essential Changes

If important entries are to be changed, the input SHOULD be verified again by a password. The users SHOULD be informed about changes through communication channels outside the web application (for example, by e-mail).

APP.3.1.A16 Comprehensive Input Validation and Output Encoding [Developer]

All data passed to a web application SHOULD be deemed potentially hazardous and filtered accordingly. All input data, as well as data flows and secondary data (e.g. session IDs), SHOULD be validated during this process. On the server, the data SHOULD be checked on a trustworthy IT

system. Erroneous input SHOULD not be handled automatically ("sanitising"). If it cannot be avoided, however, sanitising SHOULD be implemented securely in order to rule out misuse.

Output data SHOULD be encoded so that malicious code is not interpreted or executed on the target system.

APP.3.1.A17 Error Handling [Developer]

If errors occur during operation of a web application, these errors SHOULD be handled in such a way that a consistent state of the web application is guaranteed. The following items SHOULD be taken into consideration during error handling:

- Error messages SHOULD be logged.
- An initiated action SHOULD be aborted in the event of an error.
- Access to the requested resource or function SHOULD be denied as a result.

Previously reserved resources SHOULD be released within the framework of error handling. Errors SHOULD preferably be handled by the web application itself.

APP.3.1.A18 Checking Logging Data

For each web application, a concept defining how comprehensive the logging should be and how the data is to be analysed SHOULD be drawn up. Furthermore, a person SHOULD be made responsible for analysing logging data. The results of the evaluation SHOULD be submitted to the Chief Information Security Officer (CISO) or another specifically appointed employee.

APP.3.1.A19 Protection Against SQL Injections

Web applications SHOULD carefully check and filter all input and parameters before these are forwarded to the database system. Stored procedures or prepared SQL statements SHOULD be used to separate data and SQL statements. If neither stored procedures nor prepared SQL statements can be used, the SQL queries SHOULD be backed up separately.

APP.3.1.A21 Secure HTTP Configuration of Web Applications [Developer]

To protect against clickjacking attacks, the *X-FRAME-OPTIONS* directive SHOULD be set in the HTTP response headers of the web application.

An HTTP content security policy should also be used.

APP.3.1.A22 Checking Web Applications

Web applications SHOULD be checked for security issues at regular intervals. Audits SHOULD also be performed regularly. The results SHOULD be documented transparently, protected adequately and handled confidentially. Deviations SHOULD be investigated. The results SHOULD be presented to the CISO.

APP.3.1.A23 Prevention of Cross-Site Request Forgery [Developer] (CI)

The web application SHOULD support security mechanisms that allow for differentiation between intended site calls from a user and accidentally redirected commands from third parties. In this respect, it SHOULD at least be checked whether a secret token is required for accessing protected resources and functions, along with the session ID. The referrer field in the

HTTP request SHOULD also be reviewed as an additional characteristic in order to identify deliberate calls from users.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.3.1 *Web Applications* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.3.1 A20 Using Web Application Firewalls (CIA)

To ensure that data can be filtered at higher protocol levels, organisations SHOULD also use web application firewalls (WAFs). If a WAF is used, the configuration SHOULD be adapted to the web application to be protected. The configuration of the WAF SHOULD be checked following every update of the web application.

APP.3.1.A24 Preventing Resources from Being Blocked [Developer] (A)

As protection against denial-of-service (DoS) attacks, resource-intensive operations SHOULD be avoided and placed under special protection. A potential overflow of logging data SHOULD be monitored and avoided for web applications. SOAP messages SHOULD be validated according to the respective XML schema. For critical services and applications, checks SHOULD be performed to determine whether cooperation with DDoS mitigation service providers is appropriate.

Additional Information

For more information about threats and security safeguards for module APP.3.1 *Web Applications*, see the following publications, among others:

[HILWEB]	Hilfsmittel zur Nutzung des Bausteins Webanwendung [Tools for using the Web Applications module]: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Vorabversionen/Baustein_Webanwendungen_Hilfsmittel.pdf , last accessed on 05.10.2018
[OWASP]	Open Web Application Security Project (OWASP): https://www.owasp.org , last accessed on 05.10.2018
[TR02102]	Cryptographic Mechanisms: Recommendations and Key Lengths: BSI TR-02102, Federal Office for Information Security (BSI), January 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , last accessed on 13.09.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.3.1 *Web Applications*:

G 0.18 Poor Planning or Lack of Adaptation

- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.28 Software Vulnerabilities or Errors
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.36 Identity Theft
- G 0.38 Misuse of Personal Information
- G 0.39 Malware
- G 0.40 Denial of Service
- G 0.43 Attack with Specially Crafted Messages
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.28	G 0.30	G 0.32	G 0.36	G 0.38	G 0.39	G 0.40	G 0.43	G 0.46
APP.3.1.A1		X			X	X		X	X	X	X				X
APP.3.1.A2		X			X	X		X	X	X	X				X
APP.3.1.A3		X			X	X		X	X	X	X			X	X
APP.3.1.A4		X		X	X	X		X	X	X	X			X	X
APP.3.1.A5	X					X		X		X					
APP.3.1.A6		X	X	X	X	X	X	X			X	X			X
APP.3.1.A7		X			X	X		X	X	X	X		X	X	X
APP.3.1.A8	X					X	X								
APP.3.1.A9	X		X	X			X								
APP.3.1.A10	X		X	X			X								
APP.3.1.A11		X		X		X		X	X	X	X			X	X
APP.3.1.A12		X	X	X	X	X	X	X	X	X	X	X	X	X	X
APP.3.1.A13		X	X	X	X	X	X	X	X	X	X	X	X	X	X
APP.3.1.A14		X			X	X		X	X	X	X			X	X
APP.3.1.A15					X	X		X	X	X					X
APP.3.1.A16					X	X						X		X	X
APP.3.1.A17		X		X									X		
APP.3.1.A18	X					X		X		X					
APP.3.1.A19		X		X	X	X		X	X	X	X			X	X
APP.3.1.A20		X		X	X	X		X	X	X	X	X	X	X	X
APP.3.1.A21		X							X	X					X

APP.3.1.A22		X		X	X	X	X	X	X	X	X	X	X	X	X
APP.3.1.A23		X			X	X		X	X	X	X	X			X
APP.3.1.A24													X		



APP.3.2: Web Servers

Description

Introduction

A web server is a key component of any website: it accepts requests of the clients (browsers) and, if possible, returns the corresponding content. Usually, data is transmitted via the Hypertext Transfer Protocol (HTTP) or the version thereof that is encrypted with Transport Layer Security (TLS) – HTTP Secure (HTTPS). As web servers offer a simple interface between server applications and users, they are also frequently used for internal information and applications in organisations' own networks (intranets).

Web servers are (mainly) available directly on the Internet and are thus exposed to attacks. That is why they must be protected by appropriate security safeguards.

Objective

The aim of this module is to protect the web server and the information it provides.

Not in Scope

The term “web server” is used for both the software that responds to HTTP requests and the IT systems used to run such software. This module mainly addresses web server software. Security aspects of the IT systems on which web server software is installed are addressed in the modules of the SYS IT Systems layer (see SYS.1.1 *General Server*, as well as SYS.1.3 *Unix Servers*, SYS.1.2.2 *Windows Server 2012* and related modules).

Recommendations for integrating web servers into the network architecture and protecting them with firewalls are included in modules NET.1.1 *Network Architecture and Design* and NET.3.2 *Firewall*.

Dynamic content and functions beyond HTML are provided by web applications or web services. They are discussed not in the present module, but in APP.3.1 *Web Applications* and APP.3.5 *Web Services*.

The module CON.1 *Crypto Concept* describes how cryptographic keys can be managed in a secure manner.

Threat Landscape

For module APP.3.2 *Web Servers*, the following specific threats and vulnerabilities are of particular importance:

Loss of Reputation

If attackers succeed in manipulating or changing a website (defacement), this may damage the reputation of the organisation. The publication of incorrect information (erroneous product descriptions, for example) may also damage the organisation's public reputation or lead to the organisation being reprimanded. Damage may also occur if the website is not available and potential customers switch to competitors as a result.

Web Server Manipulation

An attacker may gain access to a web server in order to manipulate data. For example, the attacker could change the configuration, start additional services, install malware, or modify web content. The attacker could also substitute files made available for download with files containing malware. An attacker could also use the manipulated server in performing DDoS (distributed denial of service) attacks. If an organisation's own server is used for distributing malware, the web server may be added to blacklists and thus made unreachable for visitors.

Distributed Denial of Service (DDoS)

DDoS attacks may result in partial or total failure of a web server. In such case, users' access to corresponding web offerings will be very slow or not available at all. For many organisations, such failures can quickly become business-critical, such as when an online shop is affected.

In addition to DDoS, other types of denial-of-service attacks can be used to impair the accessibility of web offerings for specific users. For example, an attacker could make multiple incorrect login attempts in order to lock a user's account.

Loss of Confidential Data

Many web servers still use outdated cryptographic methods such as RC4 or SSL. Insufficient authentication or inappropriate encryption may result in attackers being able to read or change communications between the clients and servers, or between the servers.

Violation of Laws or Regulations

Violations of legal regulations, particularly those regarding telecommunications and data protection laws, may have legal consequences. Moreover, the web server content may violate copyright law, e.g. when images are used without obtaining the corresponding rights.

Software Vulnerabilities or Errors

If updates and patches for web servers or extensions in use are not installed or are installed too late, it may be possible to successfully attack the web server. In such cases, attackers may manipulate files or services or misuse the web server for further attacks.

Non-Existent or Insufficient Troubleshooting

If errors occur during operation of a web server, this may, for example, have an impact on its availability. The content displayed may be incomplete, or security mechanisms may fail. If errors are not handled correctly both the operation and the protection of the functions and data of a web server will no longer be ensured.

Insufficient Logging of Security-Relevant Events

If security-related events are insufficiently logged by the web server, it will not be possible to trace them or eliminate their causes at a later point in time. Critical errors and attacks, such as unauthorised changes in configurations, can thus remain undetected for a long time.

Requirements

The specific requirements of module APP.3.2 *Web Servers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Process Owner, Head of IT

Basic Requirements

For module APP.3.2 *Web Servers*, the following requirements **MUST** be implemented as a matter of priority:

APP.3.2.A1 Secure Web Server Configuration

After a web server has been installed, a secure basic configuration **MUST** be established. For this, the web server process (for example) **MUST** be assigned to a user account with minimal rights. The web server **MUST** also be executed in an encapsulated environment whenever this is supported by the operating system. The web server service **MUST NOT** have unnecessary write privileges. Modules and functions of the web server that are not required **MUST** be deactivated.

APP.3.2.A2 Protection of Web Server Files

All files on the web server, in particular scripts and configuration files, **MUST** be protected so that they cannot be read or changed without authorisation.

It **MUST** be ensured that the web server application can only access files that are located within a defined directory tree (WWW root directory). Resources outside of the WWW directory **MUST NOT** be referenced from within this directory.

Moreover, functions for listing directories **MUST** be deactivated. Files that should not be changed **MUST** be write-protected. Confidential data **MUST** be transmitted and stored in encrypted manner.

APP.3.2.A3 Protecting File Uploads and Downloads

All files published using the web server **MUST** be checked in advance for malware. In addition, residual information **MUST** be removed from documents. Retrievable files **MUST** be stored on a separate partition of the hard disk.

A maximum size for file uploads **MUST** be specified. Sufficient storage space **MUST** be reserved for uploads.

APP.3.2.A4 Logging of Events

The web server **MUST** log at least the following events:

- successful attempts to access resources
- failed attempts to access resources due to a lack of authorisations, unavailable resources or server errors
- general error messages

The logging data **SHOULD** be evaluated regularly.

APP.3.2.A5 Authentication

When clients authenticate themselves through the web server, an encrypted connection **MUST** be used (see APP.3.2.A11 *Encryption via TLS*). The password files on the web server **MUST** be protected cryptographically and stored in a manner that protects them against unauthorised access.

APP.3.2.A6 Prompt Installation of Security-Relevant Patches and Updates

Using various sources, the responsible employees **MUST** inform themselves regularly on current vulnerabilities of the web server software in use and install security-relevant updates promptly. Software updates and patches for web servers, as well as additional applications and extensions in use, **MUST** only be obtained from reliable sources and tested sufficiently before being installed or used. Before updates or patches are installed, it **MUST** always be ensured that the original state of the web server can be recovered.

APP.3.2.A7 Legal Framework Conditions for Websites

If web servers publish content or offer services for third parties, various legal framework conditions **MUST** be considered in this regard. For example, the applicable telecommunication, data protection and copyright laws **MUST** be observed. Requirements regarding accessibility in accordance with the German ordinance on barrier-free information technology **SHOULD** be considered, as well.

Standard Requirements

For module APP.3.2 *Web Servers*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

APP.3.2.A8 Planning the Use of a Web Server

In order to select suitable security safeguards for the web server, the intended use of the web server and its integration into the present IT infrastructure **SHOULD** be planned and documented. The documentation **SHOULD** also describe the information or services included in the web offerings in question, along with the corresponding target groups. The persons in charge of technical operations and web content **SHOULD** be specified.

APP.3.2.A9 Defining a Web Server Security Policy

A security policy stating the required safeguards and responsibilities SHOULD be drawn up. Furthermore, methods for obtaining information on current vulnerabilities, implementing security safeguards, and proceeding in case of security incidents SHOULD be specified.

APP.3.2.A10 Selecting an Appropriate Web Host [Head of IT]

If the web server is to be operated not by the organisation itself, but with the services of external (web hosting) services, the organisation SHOULD ensure the following when selecting a suitable partner:

- The manner in which the services are to be rendered SHOULD be contractually agreed. In this regard, security aspects SHOULD be included in writing in a service level agreement (SLA) as part of the contract.
- The design of the basic installation SHOULD be secure for all the products offered. The service provider SHOULD inform its customers of the risks in connection with additional applications and extensions (plug-ins). Furthermore, the service provider SHOULD be obligated to notify the organisation of updates for the programs in use on a regular basis.
- The service provider SHOULD regularly check and maintain the IT systems used to render its services. The service provider SHOULD be obligated to respond promptly in case of technical problems or compromised customer systems.
- The service provider SHOULD implement basic technical and organisational safeguards to protect its information domain.

APP.3.2.A11 Encryption via TLS

The web server SHOULD provide encryption via TLS (HTTPS) for all connections. If an HTTPS connection is provided, all content SHOULD be available exclusively via HTTPS. Mixed content SHOULD NOT be used.

APP.3.2.A12 Suitable Handling of Errors and Error Messages

The HTTP information and the displayed error messages SHOULD NOT show the name and the version of the web server software. It SHOULD also be ensured that the web server only provides application-specific error messages as information for users. In case of unexpected errors, the web server SHOULD switch to a secure mode.

APP.3.2.A13 Access Control for Web Crawlers

The access of web crawlers SHOULD be regulated in accordance with the robots exclusion standard. Content SHOULD be provided with access protection (see APP.3.2.A5 *Authentication*) to protect it from web crawlers that do not comply with this standard.

APP.3.2.A14 Integrity Checks and Protection Against Malware

Regular checks SHOULD be performed to ensure the continued integrity of files and web content (i.e. they have not been changed by attackers). The files SHOULD also be checked regularly for malware.

APP.3.2.A16 Penetration testing and Audits [Head of IT]

Web servers SHOULD be checked for security issues at regular intervals. Audits SHOULD also be performed regularly. The results SHOULD be documented transparently, protected adequately and handled confidentially. Deviations SHOULD be investigated. The results SHOULD be presented to the CISO.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.3.2 *Web Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.3.2.A15 Redundancy (A)

The web server SHOULD be designed to be redundant. The Internet connection of the web server and further IT systems, such as the web application server, SHOULD also be designed to be redundant.

APP.3.2.A17 Extended Authentication Methods for Web Servers (CI)

Extended authentication methods SHOULD be used, e.g. client certificates or multi-factor authentication.

APP.3.2.A18 Protection Against Denial-of-Service Attacks (A)

The web server SHOULD be monitored continuously in order to detect denial-of-service attacks early on. Furthermore, safeguards that prevent (or at least weaken) such attacks SHOULD be defined and implemented.

APP.3.2.A19 Setting Up a Web Editorial Team [Process Owner, Head of IT] (CIA)

A web editorial team SHOULD be established for maintaining web offerings. The web editorial team SHOULD include all the roles specified as persons in charge of web offerings in the concept. In cases involving extensive web offerings, a contact person for web applications SHOULD also be specified. Moreover, processes, procedures and persons in charge SHOULD be specified for any potential problems or security incidents.

Additional Information

For more information about threats and security safeguards for module APP.3.2 *Web Servers*, see the following publications, among others:

[BSITLS]	BSI action guidelines, Migration auf TLS 1.2 [Migration to TLS 1.2]: Federal Office for Information Security (BSI), Version 1.2, June 2016, https://www.bsi.bund.de/Shared-Docs/Downloads/DE/BSI/Mindeststandards/Migrationsleitfaden_Mindeststandard_BSI_TLS_1_2_Version_1_2.pdf , last accessed on 06.09.2018
[CS068]	Sicheres Webhosting: Handlungsempfehlung für Webhoster, [Secure Web Hosting: Recommendations for Action for Web Hosts], BSI publications on cyber security (BSI-CS068), Version 2.0, July 2018, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/

	downloads/BSI-CS_068.pdf, last accessed on 24.08.2018
[HVK]	High Availability Compendium: Federal Office for Information Security (BSI), November 2013, https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html , last accessed on 24.08.2018
[ISIWEB]	Sicheres Bereitstellen von Webangeboten (ISi-Webserver): [Secure Provisioning of Websites (ISi Series for Web Servers)]: Federal Office for Information Security (BSI), October 2017, https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Web-Server/web_server_node.html , last accessed on 24.08.2018
[NIST80044]	Guideline on Securing Public Web Servers: NIST Special Publication 800-44, Version 2, September 2007, https://csrc.nist.gov/publications/detail/sp/800-44/version-2/final , last accessed on 24.08.2018
[TR21022]	Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths: Part 2: Use of Transport Layer Security (TLS), Federal Office for Information Security (BSI), January 2017, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , last accessed on 24.08.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.3.2 *Web Servers*:

- G 0.11 Failure or Disruption of Service Providers
- G 0.15 Eavesdropping
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.39 Malware

G 0.40 Denial of Service

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.1 1	G 0.1 5	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 5	G 0.2 6	G 0.2 7	G 0.2 8	G 0.2 9	G 0.3 0	G 0.3 1	G 0.3 9	G 0.4 0	G 0.4 6
APP.3.2.A1				X		X	X	X										X
APP.3.2.A2				X		X	X	X										X
APP.3.2.A3				X												X	X	
APP.3.2.A4										X					X			
APP.3.2.A5		X					X	X							X			
APP.3.2.A6					X	X							X					X
APP.3.2.A7													X					
APP.3.2.A8			X								X				X			
APP.3.2.A9			X								X				X			
APP.3.2.A10	X		X										X					
APP.3.2.A11		X																
APP.3.2.A12				X					X	X								
APP.3.2.A13														X				
APP.3.2.A14																X		X
APP.3.2.A15									X							X		
APP.3.2.A16							X	X					X					
APP.3.2.A17							X	X						X				

APP.3.2.A1 8									X	X							X	
APP.3.2.A1 9			X							X								



APP.3.3: File Servers

Description

Introduction

A file server is a network server that provides files centrally for all users or clients with access authorisation. The data can be shared by users with access authorisation without transporting them, e.g. to removable storage media or by distributing them by e-mail. The data can be structured and provided in various file versions because it is available centrally. In cases involving file servers, rights can be assigned and backups created in a centralised manner.

A file server mainly manages mass-storage devices connected via interfaces such as SCSI (Small Computer System Interface) or SAS (Serial Attached SCSI). The memory is either located directly within the server's casing or connected externally. The latter is often referred to as 'directly attached storage' (DAS). A file server can be operated on normal server hardware or a dedicated appliance, e.g. a 'network attached storage' (NAS) device. For large amounts of data, central SAN storage (Storage Area Network) and SAN switches can also often be connected via HBA (Host Bus Adapters).

Objective

This module describes the specific threats to file servers and the resulting requirements for secure operation.

Not in Scope

The present module includes basic requirements which must be observed and fulfilled when operating file servers. The general and operating system-specific aspects of a server are not included in the present module. These aspects are addressed in module SYS1.1 *General Server* and in the relevant operating-system-specific modules of the *IT Systems* layer, e.g. SYS.1.3 *Unix Server* or SYS.1.2.2 *Windows Server 2012*. Furthermore, the requirements placed on storage systems and storage networks are not described. These are included in module SYS.1.8 *Storage Solutions*. Dedicated services for operating a file server, e.g. Samba, are not addressed.

Threat Landscape

For module APP.3.3 *File Servers*, the following specific threats and vulnerabilities are of particular importance:

Failure of a File Server

If a file server fails, the whole information domain (and thus important business processes of the organisation, as well) may be affected. In addition to the users, applications may depend on

data from the file server to function properly. If data and services are not available, it may not be possible to meet deadlines and essential business processes will fail (among other potential problems). In addition, if no business continuity management concept has been implemented, restoration times may increase further. In many cases, this will result in financial losses of the organisation or impacts on other organisations.

Insufficient Capacity of the File Server

If the line connection or the storage capacity of the file server is not sufficient, the access times may increase or there may be storage bottlenecks. This can result, for example, in the risk of employees becoming frustrated and starting to store data locally due to long waiting times. This means it will no longer be possible to trace where data is stored and who owns it.

Insufficient Checking of Stored Files

If a file server is not sufficiently included in an organisation's malware protection concept, attackers may place malware on the file server unnoticed. This may result in unauthorised access to or manipulation of data on the file server. However, there are also security risks for all the devices and applications that access the file server. Malware may thus spread very quickly throughout the organisation (for example).

Non-Existent or Insufficient Access Authorisation Concept

If access authorisations and approvals are not designed and assigned properly, unauthorised third parties might access data. Attackers could thus change, delete, or copy data.

Unstructured Data Organisation

If the storage structure is not specified or employees do not comply with it, data can be stored on the file server in a confusing and uncoordinated manner. This will result in a variety of problems, such as wasted storage space due to redundancy, unauthorised access where files are located in directories or file systems that are made accessible to third parties or inconsistent versions.

Inappropriate Siting of the File Server

If file servers are positioned in easily accessible locations, attackers may access their components and stored data directly, e.g. by removing and taking along drives. In addition, it will be easy to steal entire NAS systems of smaller sizes. Furthermore, it will be possible for an attacker to circumvent access restrictions directly on the file server in order to read sensitive data. Once the attacker has corresponding access, it will be possible to install malware and threaten the security of the whole network.

Non-Existent or Insufficient Backup Concept

If a file server fails completely, individual components are defective, or an employee inadvertently deletes files, important data can get lost without a functioning backup. In addition, if no RAID (Redundant Array of Independent Disks) is used, the failure of individual storage media will have a direct impact on the operation due to files no longer being available.

Requirements

The specific requirements of module APP.3.3 *File Servers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User, Building Services

Basic Requirements

For module APP.3.3 *File Servers*, the following requirements **MUST** be implemented as a matter of priority:

APP.3.3.A1 Suitable Siting [Building Services]

File servers **MUST NOT** be operated in office rooms or as personal computers. They **MUST** be placed at locations which can only be accessed by authorised persons. In addition, a vibration-free or shock-free environment **MUST** be ensured for file servers. File servers with further functions (such as NAS systems combined with a WLAN access point) or direct connections for memory cards **MUST** also be placed at suitable locations. Furthermore, a secure power supply and compliance with the manufacturer's environmental temperature and air humidity specifications **MUST** be ensured.

APP.3.3.A2 Use of RAID systems

Plans **MUST** be made as to whether the file server will use a RAID system. A decision against such a system **MUST** be documented comprehensibly. If a RAID system is to be used, the following **MUST** be decided:

- the RAID level that should be used for logically combining the storage media
- the length of time allowed for a RAID rebuild process
- whether to use a software or a hardware RAID

The RAID levels **MUST** correspond to the current state of the art. In cases involving a hardware RAID, the design of the RAID controller **SHOULD** be redundant. Hot spare hard disks **SHOULD** be available in a RAID.

APP.3.3.A3 Use of Anti-virus Programs

Depending on the operating system and other available protection mechanisms, the file server **MUST** be integrated into the concept of the organisation for protection against malware. The anti-virus program used **MUST** regularly check the files approved via the file server. In addition to real-time and on-demand scans, the employed solution **MUST** also be able to search for malware in compressed files. In addition, it **SHOULD** also be able to check encrypted files.

Before being stored on a storage medium, all files **MUST** be checked for malware by the anti-virus solution. Both the virus signatures and the anti-virus software itself **MUST** be updated continuously. Care **MUST** be taken to ensure that users are not able to make any security-related changes to the settings of the anti-virus solution.

APP.3.3.A4 Regular Backups

All data available on the file server **MUST** be backed up regularly. A backup concept that defines the backup intervals (along with other aspects) **MUST** be drawn up. Moreover, a backup **MUST** be made if something is installed or newly configured on the file server. Recovery of all backed-up data **MUST** be possible at any time. Here, the maximum recovery time **SHOULD** be determined and considered in the backup concept.

APP.3.3.A5 Restrictive Granting of Access Rights

Access rights to files managed by the file server **MUST** be granted restrictively. It **MUST** be ensured that every user may only access the data required to perform his/her tasks. System directories and files **MUST NOT** be shared with unauthorised users.

Regular checks **MUST** be performed to ensure that the access authorisations are up to date and comply with the security policy. Furthermore, there **MUST** be a defined process for creating new authorisations and changing or withdrawing existing authorisations. All access rights **MUST** be documented comprehensibly.

Standard Requirements

For module APP.3.3 *File Servers*, the following requirements correspond to the state-of-the-art technology together with the basic requirements. They **SHOULD** be implemented as a matter of principle.

APP.3.3.A6 Purchasing a File Server

Before purchasing a file server, a requirements list **SHOULD** be drawn up that can be used to evaluate the products available on the market. Performance, storage capacity, bandwidth, and the number of people who will be using it **SHOULD** be considered when purchasing the file server.

APP.3.3.A7 Selecting a File System

A requirements list for assessing the file systems **SHOULD** be drawn up. The file system **SHOULD** provide a journaling function in order to ensure transaction security. Moreover, it **SHOULD** have a protection mechanism that prevents two users or applications from accessing a file with write permissions at the same time. A file system that does not exceed a specified overhead limit **SHOULD** be selected. Distributed file systems **SHOULD** be selected for high-availability solutions.

APP.3.3.A8 Structured Data Organisation [User]

A structure for organising data **SHOULD** be specified. Users **SHOULD** be informed regularly about the structured data organisation required. The data to be stored locally and on the file server **SHOULD** be specified in writing. Program and work files **SHOULD** be stored separately. Regular checks **SHOULD** be performed to ensure compliance with the requirements for structured data organisation.

APP.3.3.A9 Secure Storage Management

All storage resources of the file server (e.g. hard disks, flash memory, tape drives) SHOULD be catalogued. In addition, regular checks SHOULD be performed to ensure that storage memory still works as intended. Substitute storage SHOULD be available in order to respond quickly in case of bottlenecks.

If a memory hierarchy (primary, secondary and tertiary memory) has been established, (partially) automated memory management SHOULD be used. If data is distributed automatically, the proper functioning of the distribution method SHOULD be checked manually at regular intervals.

Furthermore, the employed storage memory SHOULD be integrated into the logging concept of the information domain. The following events SHOULD be logged at minimum:

- activities (modifying, adding or deleting data)
- unauthorised attempts to access data
- changes to access rights

APP.3.3.A10 Regular Tests of the Backup or Recovery Concept

Regular tests SHOULD be performed to determine whether the backup and recovery are functioning properly. A time schedule for this SHOULD be created. Sufficient resources for planning, designing and performing the tests SHOULD be provided.

The results SHOULD be documented sufficiently. Any defects discovered SHOULD result in a review of the backup concept.

APP.3.3.A11 Using Quotas

Consideration SHOULD be given to configuring quotas. As an alternative, mechanisms of the file or operating system in question SHOULD be used that warn the users or only grant write privileges to the system administrator if the hard drive capacity reaches a specific level.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.3.3 *File Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.3.3.A12 Data Encryption (CI)

All data on the file server SHOULD be encrypted. To achieve this, the storage media SHOULD be fully encrypted. It SHOULD be ensured that the virus protection program in question can scan encrypted files for malware. Cryptographic keys SHOULD be generated securely and kept separate from the data (see also CON.1 *Crypto Concept*).

APP.3.3.A13 Replicating Between Locations (A)

For high-availability systems, data SHOULD be replicated appropriately on several storage media. In addition, data SHOULD be replicated between independent devices and independent

locations. A suitable replication mechanism SHOULD be selected for this. Sufficiently accurate time services SHOULD be used and operated so that the replication can work as intended.

APP.3.3.A14 Using Error Correction Codes (I)

Error detection and correction procedures SHOULD be used in general, e.g. at the file system level. The required redundant bits SHOULD be included in related planning. It SHOULD be taken into account that, depending on the method used, errors can only be detected with a certain probability and can only be removed to a limited extent.

Additional Information

For more information about threats and security safeguards for module APP.3.3 *File Servers*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[HVK]	High Availability Compendium: Federal Office for Information Security (BSI), November 2013, https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/Hochverfuegbarkeit/HVKompendium/hvkompendium_node.html , last accessed on 24.08.2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 15.11.2017

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.3.3 *File Servers*:

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.1 4	G 0.1 6	G 0.1 8	G 0.1 9	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 5	G 0.2 6	G 0.2 7	G 0.3 0	G 0.3 1	G 0.3 2	G 0.3 9	G 0.4 0	G 0.4 3	G 0.4 4	G 0.4 5	G 0.4 6
APP.3.3.A1		X						X	X								X		
APP.3.3.A2								X	X									X	
APP.3.3.A3	X	X		X	X	X	X							X	X	X		X	X
APP.3.3.A4								X	X									X	X
APP.3.3.A5				X	X	X	X				X	X	X						X
APP.3.3.A6			X					X	X	X									
APP.3.3.A7																		X	X
APP.3.3.A8				X						X								X	
APP.3.3.A9			X	X	X		X	X	X	X	X	X	X		X			X	X
APP.3.3.A10			X											X				X	
APP.3.3.A11								X		X									
APP.3.3.A12	X			X		X					X	X				X			
APP.3.3.A13								X	X									X	X
APP.3.3.A14								X	X									X	X



APP.3.4: Samba

Description

Introduction

Samba is a freely available and full-featured Active Directory Domain Controller (AD DC) that is able to provide authentication, file and print services as a means of facilitating interoperability between Windows and Unix. Samba combines many different protocols and technologies. They include the Server Message Block (SMB) protocol, which is also known by its newer name, the Common Internet File System (CIFS). The term "Samba server" refers to servers running Samba. Usually, these are Linux servers.

If *Samba* is designed and configured properly, the application will interact with a Windows client or server as if it were a Windows system itself.

Objective

The aim of this module is to show how Samba can be used in a secure manner in organisations and how information provided by Samba can be protected.

Not in Scope

This module deals with Samba as an authentication, file and print service. As Samba is usually used on Linux servers, where it reproduces known services from the world of Windows servers, the security aspects of the modules SYS.1.1 *General Server* and SYS.1.3 *Unix Servers* must be considered. Security requirements for printers, file servers or directory services, however, are not part of the present module; they are described in the modules SYS.4.1 *Printers, Copiers, and All-in-One Devices*; APP.2.1 *General Directory Service*; and APP.3.6 *DNS Servers*, as well as in APP.2.3 *OpenLDAP* (even when Samba-internal DNS and LDAP services are used). Furthermore, the modules APP.3.3 *File Servers* and APP.2.2 *Active Directory* must be considered due to the Samba functions involved.

Threat Landscape

For module APP.3.4 *Samba*, the following specific threats and vulnerabilities are of particular importance:

Eavesdropping on Unprotected Samba Communication Links

If attackers eavesdrop on unprotected Samba communication links, information can be intercepted and misused. Protocols without comprehensive security characteristics are often used for data transfers between Linux servers, Windows servers and clients. As a result, both authen-

tication data and payloads are accessible to third parties and can be misused by unauthorised persons. This may lead to leaks of sensitive information at an organisation.

Incorrect Logging in Samba

Non-existent or inappropriately designed logging in Samba can result in security problems. Without appropriate logging, errors or attacks can remain undetected and preventive actions and indicators for early warning systems cannot be defined.

Improper Contingency Planning in Samba

Deficiencies in contingency planning can also result in longer Samba downtimes. For example, a reinstallation that is required after an attack may be delayed if installation packages are not available. Available installation packages may also lead to undesired results if no version management has been used for the configuration files or neither compiling nor installation options for the Samba servers are available.

Lack of Adaptation of Samba

To demonstrate some of the capabilities of the Samba server and provide administrators with a quick introduction, the smb.conf configuration file is created with default settings during the installation of the Samba server. The default options in this file can be used for starting the Samba server. If this file is used incautiously without further settings, this may result in significant vulnerabilities. Even if the file is changed, errors can occur that could result in confidential information being viewed or the security, availability and performance of a Samba server's services being compromised.

Software Vulnerabilities or Errors in Samba

Samba is free software that is being created and developed further by a community. This means that the uniform quality of the source code cannot be guaranteed. This may result in software vulnerabilities or errors, and thus in serious vulnerabilities in the application or all the IT systems connected to it. Attackers may use such vulnerabilities for various attacks. For example, they can smuggle in malware and possibly gain unauthorised access to sensitive information such as confidential data or documents and login data. Moreover, attackers may use vulnerabilities to manipulate IT systems, which may render them inaccessible or no longer fully functional.

Unauthorised Use or Administration of Samba

Unauthorised persons may use applications or systems to obtain and manipulate confidential information or cause malfunctions so that they can administrate Samba without authorisation. It is particularly critical if configuration tools such as the Samba Web Administration Tool (SWAT) are used. SWAT was an integral part of Samba until version 4, but was given low priority by Samba's developers. For this reason, weaker security mechanisms (or none at all) have been implemented in some cases; HTTPS was not supported, for example.

Incorrect Administration of Samba

If the administrators are not sufficiently familiar with the functions, components, options and configuration settings of Samba, this may result in serious complications. For example, incorrect configurations of DNS or user and rights management may allow unauthorised persons to

access resources. Furthermore, this may result in operational interruptions or the disclosure of sensitive information.

Malware in Samba Service Environments

If Samba is used as a file server on Linux systems, the server itself will not be directly vulnerable to Windows malware. However, malware of this kind can be present in infected files stored on such servers. The Samba system can then distribute and actively spread these infected files to all the connected Windows clients.

Data Loss with Samba

Data loss can have a significant impact on the use of IT. When business information is destroyed or corrupted, this can cause delays in business processes and specialised tasks, or even prevent their execution. In the case of Samba, it should be considered that the properties of the file systems in Windows and Unix differ significantly (for example). That is why it cannot always be assumed that access rights will still be in place in Windows. This may also result in the loss of information on alternate data streams (ADS) and DOS attributes.

Loss of Integrity of Sensitive Information with Samba

When the integrity of information is violated, a number of problems can arise. In the simplest case, it may be impossible to read the information, which means it can no longer be processed. Samba stores important operating data in databases in the Trivial Database (TDB) format. If these databases are not handled with sufficient performance capability and consistency by the operating system, they can cause problems when Samba services are used.

Requirements

The specific requirements of module APP.3.4 *Samba* are listed below. In general, it is the responsibility of the IT Operation Department to fulfil the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring all requirements are met and verified according to the security concept agreed upon.

Module Owner	IT Operation Department
Further Roles	Head of IT

Basic Requirements

For module APP.3.4 *Samba*, the following requirements **MUST** be implemented as a matter of priority:

APP.3.4.A1 Planning the Use of a Samba Server [Head of IT]

The introduction of a Samba server **MUST** be carefully planned and regulated. The tasks to be performed by the Samba server and the corresponding operating mode of the server, as well as the Samba components and any further components required, **MUST** be defined on the basis of the application scenario.

If the CTDB (Cluster Trivia Data Base) cluster solution is to be used, the introduction of Samba MUST be planned properly. If Samba will provide Active Directory (AD) services for Linux and Unix systems, as well, the implementation MUST be planned carefully and the installation MUST be tested. Furthermore, the authentication procedure for AD MUST be designed and implemented carefully. The implementation and the order in which the Stackable Virtual File System (VFS) modules are executed MUST be designed carefully, and the implementation MUST be documented.

If IPv6 is used in Samba, this MUST be planned carefully and also checked for error-free integration in a test environment that closely resembles the operating environment.

APP.3.4.A2 Secure Basic Configuration of a Samba Server

After installing the Samba server, the service MUST be configured in a secure manner. Among other aspects, the access control settings and settings that impact server performance MUST be adapted. It MUST be ensured that access authorisations are specified individually for every user.

In general, it MUST be ensured that only select users and user groups are allowed to connect to the Samba service and that users may only access the information corresponding to their authorisation levels.

Samba MUST be configured so that connections can only be accepted by secure hosts and networks and it only connects to secure network addresses. Changes to the configuration SHOULD be documented carefully so that it is possible at any time to determine who made which changes and for what reasons. In such cases, the syntax MUST be checked for correctness after every change.

Additional software modules such as SWAT MUST NOT be installed.

Standard Requirements

For module APP.3.4 *Samba*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

APP.3.4.A3 Secure Configuration of a Samba Server's Operating System

Databases in the Trivial Database (TDB) format SHOULD NOT be stored on a partition that uses ReiserFS as its file system. If a netlogon share is configured, unauthorised users SHOULD NOT be able to modify any files in the share.

The operating system of the Samba server SHOULD support access control lists (ACLs) in connection with the file system used. In addition, it SHOULD be ensured that the file system is integrated with the appropriate parameters.

The default settings of SMB Message Signing SHOULD be maintained unless they are contrary to the existing security policies in the information domain. A local packet filter SHOULD be used to block ports on which the Samba server should not be accessible.

Kerberos SHOULD be used to avoid the vulnerabilities pertaining to NT LAN Manager (NTLM), NTLMv2, and excessive network loads. If Kerberos is used for authentication, the central time server SHOULD be installed locally on the domain controller. The NTP service SHOULD be hardened so that only authorised clients can request the time.

APP.3.4.A4 Ensuring the NTFS File Properties on a Samba Server

When using a version of Samba that cannot map the alternate data streams (ADS) in the New Technology File System (NTFS), it SHOULD be ensured that no file system objects contain an ADS with important information before copying or moving them from one type of system to another.

APP.3.4.A5 Secure Configuration of a Samba Server's Access Controls

The default parameters used by Samba to map DOS attributes to the Linux file system SHOULD NOT be used. Instead, Samba should be configured to save DOS attributes and the status indicators for inheritance (flag) in extended attributes. The shares SHOULD only be managed via the registry.

Furthermore, the effective access authorisations for the shares of the Samba servers SHOULD be checked regularly, along with the log files.

APP.3.4.A6 Secure Configuration of Winbind in Samba

The use of Winbind SHOULD be planned and regulated carefully. The operating system of the server SHOULD include a user account with all group memberships for each Windows domain user. If this is not possible, Winbind SHOULD be used to convert domain user names into unique Linux user names. Here, it SHOULD be ensured that conflicts between local Linux users and domain users are prevented.

Furthermore, the PAM (pluggable authentication modules) SHOULD be integrated.

APP.3.4.A7 Secure Configuration of DNS in Samba

If Samba is to be used as a DNS server, the implementation SHOULD be planned carefully and tested in advance.

As Samba supports various AD integration modes, the DNS settings SHOULD be set in accordance with the Samba usage scenario at hand. If Samba is used as the primary AD DC, the DNS service SHOULD be installed on the Samba server and configured carefully.

APP.3.4.A8 Secure LDAP Configuration in Samba

If the users are managed with LDAP in Samba, this SHOULD be planned and documented carefully. The access authorisations to LDAP SHOULD be controlled by means of ACLs.

APP.3.4.A9 Secure Configuration of Kerberos in Samba

The Heimdal Kerberos Key Distribution Center (KDC) implemented by Samba SHOULD be used for authentication. It SHOULD be ensured that the Kerberos configuration file specified by Samba is used. Only sufficiently secure encryption methods SHOULD be used for Kerberos tickets.

APP.3.4.A10 Secure Use of External Programs on a Samba Server

As external programs represent points of entry for attackers, it SHOULD be ensured that Samba only calls verified and trustworthy external programs.

APP.3.4.A11 Secure Use of Communication Protocols When Using a Samba Server

Windows clients SHOULD only use protocols that are truly needed in order to ensure a reliable network. If NetWare systems must access the Samba server, it SHOULD be considered that the

Internetwork Packet Exchange (IPX) is required. If IPv6 is used, any required particularities SHOULD be considered.

APP.3.4.A12 Training Samba Server Administrators

Administrators SHOULD receive training on the specific areas of Samba used – user authentication and rights models for Windows and Unix, for example, but also on ACLs and ADS for NTFS.

APP.3.4.A13 Regular Backups of Important Samba Server Components

All system components required to recover a Samba server SHOULD be included in the organisation-wide backup concept. The account information of all the back ends in use SHOULD also be considered. In addition, all TDB files should be backed up. Furthermore, the registry SHOULD be backed up if it has been used for shares.

Configuration data, status information and system files SHOULD be compatible with each other.

APP.3.4.A14 Creation of a Contingency Plan for Samba Server Failure

The required installation packets and information SHOULD be stored at a specified location to enable the Samba server to be reinstalled quickly in an emergency. It SHOULD be ensured that they are available at any time. The Samba configuration documentation SHOULD always be up to date and comprehensible.

Depending on the server role and the availability requirements, the Samba server SHOULD be tested in terms of whether it can be recovered and how long this takes. The contingency plan SHOULD be improved on the basis of the results.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.3.4 *Samba* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.3.4.A15 Encryption of Data Packets in Samba (CI)

Data packets SHOULD be encrypted with the encryption methods integrated into SMB3 in order to ensure the integrity and confidentiality of the packets during transmission.

Additional Information

For more information about threats and security safeguards for module APP.3.4 *Samba*, see the following publications, among others:

[SAMBA]	Samba: https://www.samba.org/ , last accessed on 05.10.2018
[UBUNTU]	ubuntuuser: Wiki / Samba, https://wiki.ubuntuusers.de/Samba , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.3.4 *Samba*:

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.39 Malware

G 0.40 Denial of Service

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.15	G 0.18	G 0.19	G 0.28	G 0.30	G 0.31	G 0.39	G 0.40	G 0.45	G 0.46
APP.3.4.A1		X				X		X		
APP.3.4.A2		X				X	X	X		
APP.3.4.A3		X				X		X		
APP.3.4.A4		X				X			X	
APP.3.4.A5		X	X			X				X
APP.3.4.A6		X				X				
APP.3.4.A7	X				X					
APP.3.4.A8		X		X		X				
APP.3.4.A9	X	X	X			X				
APP.3.4.A10		X				X	X	X	X	
APP.3.4.A11		X							X	
APP.3.4.A12		X								X
APP.3.4.A13	X		X							
APP.3.4.A14								X		
APP.3.4.A15	X		X							X



APP.3.6: DNS Servers

Description

Introduction

This module examines the basic security features of the Domain Name System (DNS) and the servers required for this. DNS is a network service used to convert host names of IT systems into IP addresses. Usually, for a host name, the corresponding IP address is searched for (forward resolution). If, however, the IP address is known and the host name is searched for, this is referred to as reverse resolution. DNS can be compared to a telephone book which does not resolve names into telephone numbers, but into IP addresses. Which names belong to which IP addresses is managed in the domain name space. The domain name space has a hierarchical structure and is provided by DNS servers. DNS servers manage the domain name space in the Internet, but are often also used within the organisation's internal network. On the users' computers, so-called resolvers are installed by default, by means of which the requests are sent to DNS servers and which return information on the domain name space as a response. In the proper meaning of the word, the term "DNS server" refers to the software used, but it is mostly also used as a synonym for the computer on which this software is run.

DNS servers are differentiated according to their tasks, wherein there are two basic types as a matter of principle: advertising DNS servers and resolving DNS servers. The task of advertising DNS servers is usually to process requests from the internet. Resolving DNS servers, however, process requests from the internal network.

A failure of a DNS server may have severe consequences on the operation of an IT infrastructure. In this, it is not the failed DNS system that is immediately problematic, but the resulting limitation of DNS-based services. Web servers, email servers may no longer be available and remote maintenance may be out of function. Since DNS is required by a very large number of network applications, RFC 1034 specifies that at least two authoritative DNS servers (advertising DNS servers) must be operated for every zone.

Objective

This module describes the DNS server-specific threats and the requirements for secure operations resulting from this.

Not in Scope

The present module includes basic requirements to be considered and complied with when an organisation operates a DNS server. In this, the focus is on the availability of DNS servers, the integrity of the information transmitted, and on issues that may occur when DNS servers are operated. General and operating system-specific aspects of a server are not included in the present module, but are addressed in the module SYS.1.1 *General Server* and in the relevant op-

erating system-specific modules of the *SYS IT Systems* layer, e.g. *SYS.1.3 Unix Servers* or *SYS.1.2.2 Windows Server 2012*.

Threat Landscape

The following specific threats and vulnerabilities are of particular importance for the module *APP.3.6 DNS Servers*:

Failure of the DNS Server

If a DNS server fails, the entire IT operations may be affected by this. Since clients and other servers of the organisation are no longer able to resolve internal and external addresses, no data connections can be established any more. Even external IT systems, e.g. of mobile employees, customers, and business partners, are not able to access the organisation's servers, which normally disturbs essential business processes.

Inadequate Line Bandwidth

If the bandwidth is insufficient for a DNS server, the times required for accessing internal and external services may be prolonged. As a consequence, these might only be used to a limited extent or not at all. Likewise, attackers may find it easier to overload the DNS server by means of a denial of service attack (DoS attack).

Lack of or Inadequate Planning of the Use of DNS

Planning errors often turn out to be particularly serious, since they may easily create comprehensive vulnerabilities. If the use of DNS is planned not at all or only insufficiently, this may result in problems and vulnerabilities during live operation. If, for example, the firewall rules allowing DNS traffic in the network are defined too generously, this might allow for an attack under certain circumstances. However, if the rules have been formulated too restrictively, legitimate clients are not able to send requests to the DNS servers and are impaired when using services such as email, FTP, or the like.

Incorrect Domain Information

Even if the use of DNS has been planned carefully and, thus, all security-relevant aspects have been taken into consideration, this is not sufficient if domain information that is semantically and/or syntactically incorrect is created. For example, if a host name is assigned an incorrect IP address, data is missing, or characters that are not permitted are used, or the forward and reverse resolutions are inconsistent. If domain information contains errors, services using this information only function to a limited extent due to the incorrect information.

Incorrect Configuration of a DNS Server

Security-critical default settings, self-configured security-critical settings, or incorrect configurations may cause a DNS server to function improperly. For example, if a resolving DNS server has been configured to accept recursive requests without any limitations, i.e. both from the internal LAN and from the Internet, the availability of the server may be impaired significantly due to the increased load. Additionally, the server might become susceptible to DNS reflection attacks as a consequence.

Likewise, incorrectly configured DNS servers are subject to the threat that the zone transfers are not limited to authorised DNS servers. As a consequence, every host having the option of

sending a request to the DNS server may read out the entire domain information of these servers. The data obtained this way may facilitate future attacks.

DNS Manipulation

A DNS cache poisoning attack has the objective of the attacked computer storing improper assignments of IP addresses and names. In so doing, the fact that DNS servers cache received domain information for a certain period of time is exploited. Falsified data may spread widely this way. If corresponding requests are sent to the manipulated DNS server, this server will return the falsified data. The receiver of the response caches the falsified data and its cache is therefore also “poisoned”. The length of time for stored data to expire can be configured (time to live, TTL). If a manipulated address is requested from the resolving DNS server, it will not send a request to a different DNS server until the set length of time has expired. This way, it is possible for manipulated DNS information to persist for a long time, although they have already been corrected on the DNS server originally attacked. If, for example, an attacker is able to take the name resolution for a domain by manipulating the entries in such a way that requests are sent to his DNS servers, all sub-domains are automatically affected by this. DNS cache poisoning attacks are often performed with the objective of diverting requests to malicious servers.

DNS Hijacking

DNS hijacking is a type of attack used to route the communications between advertising DNS servers and resolvers via the IT system of an attacker. By using this man-in-the-middle attack, the attacker can intercept and record the communications between the servers. The far greater threat, however, is that a successful attacker is able to change any traffic of the two communication partners in any way. If a request is sent by the resolver of a client IT system to a DNS server after a DNS hijacking attack has been completed successfully, the attacker may, for example, modify the assignment of name and IP address. DNS hijacking can also be combined with other forms of attack; phishing in particular is ideal in this case.

DNS DoS

When a DoS attack on a DNS server is carried out, the number of requests sent to this server is so high that the network connection to the DNS server or the DNS server itself will become overloaded. In general, the requests are sent using bot networks to achieve the required data rate. A DNS server that has become overloaded in this manner can no longer respond to any legitimate requests.

DNS Reflection

A DNS reflection attack is a DoS attack not aiming at the DNS the requests are sent to, but the receiver of the responses. It takes advantage of the fact that certain requests generate a relatively large amount of response data. Here, it is possible to achieve an amplification factor of 100 and higher. This means that the response, measured in bytes, is at least 100 times larger than the request. Due to the number and size of the responses, the network bandwidth or the computer itself will become overloaded beyond its capacity. Thus, any technical IT component may be the target of the attack (see 2.8 *DNS DoS*). DNS reflection attacks are favoured by open resolvers.

Requirements

The specific requirements of the module APP.3.6 *DNS Servers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief

Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Head of IT, Supervisor

Basic Requirements

The following requirements **MUST** be implemented for the module APP.3.6 *DNS Servers* as a matter of priority:

APP.3.6.A1 Planning the DNS deployment

Since a working name resolution is a prerequisite for many applications and hence for smooth operations, DNS servers **MUST** be planned carefully. In this, it **MUST** initially be defined how the network server DNS is to be configured and which domain information is sensitive. It **MUST** also be planned how DNS servers are to be incorporated into the network of the information domain. The decisions made **MUST** be documented.

APP.3.6.A2 Deployment of redundant DNS servers

Advertising DNS servers (external requests) **MUST** be designed redundantly. As a consequence, there **MUST** be at least one additional secondary DNS server for every advertising DNS server.

APP.3.6.A3 Use of separate DNS servers for internal and external requests

Advertising DNS servers (external requests) and resolving DNS servers (internal requests) **MUST** be separated on the server side. The resolvers of the internal IT systems **MAY ONLY** use the internal resolving DNS servers to resolve names.

APP.3.6.A4 Secure basic configuration of a DNS server

A resolving DNS server **MUST** be configured to only accept requests from the internal network. If it sends requests, it **MUST** use random source ports. If DNS servers delivering forged domain information are known, the resolving DNS server **MUST** be prevented from sending requests to these DNS servers. An advertising DNS server **MUST** be configured to always iteratively handle requests from the Internet.

It **MUST** be ensured that DNS zone transfers between primary and secondary DNS servers work. Additionally, zone transfers **MUST** be configured to be only possible between primary and secondary DNS servers. In order to protect zone transfers, these **MUST** be limited to certain IP addresses. The version of the DNS server product used **MUST** be hidden.

APP.3.6.A5 Prompt installation of security-relevant patches and updates

The employees in charge **MUST** regularly obtain information from different sources regarding newly published vulnerabilities in the DNS server product used and **MUST** install security-relevant updates in a timely manner. However, a test system **MUST** be used in advance to check whether the security updates are compatible and do not cause any errors. As long as no patches are available in the event of known vulnerabilities, other appropriate safeguards **MUST** be im-

plemented in order to protect the DNS servers. Prior to installing a patch, the zone and configuration files **MUST** be backed up.

APP.3.6.A6 Securing dynamic DNS updates

In order to be able to securely use dynamic updates, **ONLY** legitimate IT systems **MAY** change domain information. Furthermore, it **MUST** be specified which domain information may be changed by the IT systems.

APP.3.6.A7 Monitoring of DNS servers

In order to smoothly operate DNS servers and identify possible failures or anomalies, the servers **MUST** be monitored continuously. Furthermore, the utilisation of the DNS servers **MUST** be monitored in order to be able to timely adapt the performance capacity of the hardware. Moreover, all security-relevant events associated with DNS servers **MUST** be logged.

APP.3.6.A8 Administration of domain names [Head of IT]

It **MUST** be ensured that the registrations for all of the domains that an organisation uses are extended regularly and in good time. An employee **MUST** be appointed to be in charge of administering the Internet domain names. If an Internet service provider is charged with the domain administration, it **MUST** be ensured that the organisation retains control of the domains.

APP.3.6.A9 Creation of a business continuity plan for DNS servers

A business continuity plan **MUST** be drawn up for DNS servers. This plan **MUST** be integrated into the already existing business continuity plans of the organisation. Furthermore, the plan **MUST** describe a backup concept for the zone and configuration files that **MUST** be integrated into the existing backup concept of the organisation. The business continuity plan **MUST** also include a plan to restore service to DNS servers.

Standard Requirements

Together with the Basic Requirements, the following requirements correspond to the state-of-the-art technology for the APP.3.6 *DNS Servers* module. They **SHOULD** be implemented as a matter of principle.

APP.3.6.A10 Selection of a suitable DNS server product

When acquiring a DNS server product, it **SHOULD** be ensured that it can be used to appropriately implement all security requirements of the organisation. The product **SHOULD** have been tried and tested sufficiently in practice and support the current RFC standards. It **SHOULD** support the person in charge regarding the process of creating syntactically correct master files. Furthermore, sufficiently trained personnel **SHOULD** be available for the selected DNS server product.

APP.3.6.A11 Sufficient capacity of the DNS servers

Since the hardware of a DNS server influences the performance of the entire system, it **SHOULD** have sufficient capacity. Likewise, the hardware **SHOULD** only be used for operating one DNS server. Likewise, the network connection of the DNS servers **SHOULD** have sufficient capacity.

APP.3.6.A12 Training of the persons in charge [Supervisor, Head of IT]

Training measures SHOULD be performed in order to make sure that the persons in charge are familiar with the individual configuration options and security-relevant aspects of the DNS servers.

APP.3.6.A13 Limitation of the visibility of domain information

The name space of an information domain SHOULD be divided into a public and an internal organisational area. The public part SHOULD only include such domain information required by services that are to be available from external sources. IT systems in the internal network SHOULD not be assigned any DNS names that may be resolved from external sources if they have a public IP address.

APP.3.6.A14 Location of the name servers

Primary and secondary advertising DNS servers SHOULD be located in different network segments.

APP.3.6.A15 Analysis of the log data

The log files of the DNS server as well as of the underlying operating system SHOULD be checked and reviewed at regular intervals.

APP.3.6.A16 Integration of a DNS server in a “P-A-P” structure

The DNS servers SHOULD be integrated in a “packet filter – application level gateway – packet filter” (P-A-P) structure (see also NET.3.2 *Firewall*): the advertising DNS server SHOULD be placed in a demilitarised zone (DMZ) of the outer packet filter in this case. The resolving DNS server SHOULD be installed in a DMZ of the internal packet filter.

APP.3.6.A17 Use of DNSSEC

The DNS protocol extension DNSSEC SHOULD be enabled both on resolving DNS servers and on advertising DNS servers. The Key-Signing-Key (KSK) and Zone-Signing-Key (ZSK) keys used in the course of this SHOULD be changed at regular intervals.

APP.3.6.A18 Advanced securing of zone transfers

In order to secure zone transfers more strongly, transaction signatures (TSIG) SHOULD be used additionally.

APP.3.6.A19 Disposal of DNS servers

If a DNS server is discharged, all storage media of the server SHOULD be deleted securely. Furthermore, the DNS server SHOULD be deleted both from the domain name space and the network system.

Requirement in Case of Increased Protection Needs

Generic suggestions for module APP.3.6 *DNS Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.3.6.A20 Review of the business continuity plan for feasibility (A)

The business continuity plan SHOULD be checked regularly for feasibility.

APP.3.6.A21 Hidden master (CIA)

In order to make attacks on the primary advertising DNS server more difficult, a so-called hidden master arrangement SHOULD be performed.

APP.3.6.A22 Connection of the DNS servers via different providers [Head of IT] (IA)

Externally available DNS servers SHOULD be connected using different providers.

Additional Information

For more information about threats and security measures for the APP.3.6 *DNS Servers* module, see the following publications, among others:

[BSICS055]	Sichere Bereitstellung von DNS-Diensten:: Handlungsempfehlungen für Internet-Service-Provider (ISP) und große Unternehmen, BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 055), Version 1.0, April 2013, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_055.pdf , last accessed on 05.10.2018
[BSIDNSSEC]	Umsetzung von DNSSEC – Handlungsempfehlungen zur Einrichtung und zum Betrieb der Domain Name Security Extensions, BSI-Veröffentlichungen zur Cyber-Sicherheit (BSI-CS 121), June 2015, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Umsetzung_von_DNSSEC.html , last accessed on 05.10.2018
[ISILANA]	Sichere Anbindung von lokalen Netzen an das Internet (ISi-LANA): Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 2.1, August 2014 https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html , last accessed on 05.10.2018
[NIST800-81-2]	Secure Domain Name System (DNS) - Deployment Guide: NIST Special Publication 800-81-2, September 2013 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are important for the module APP.3.6 *DNS Servers*:

G 0.9 Failure or Disruption of Communication Networks

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.40 Denial of Service
- G 0.43 Attack with Specially Crafted Messages
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.9	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.40	G 0.43	G 0.45	G 0.46
APP.3.6.A1	X	X																
APP.3.6.A2								X	X	X					X			
APP.3.6.A3						X	X				X				X			
APP.3.6.A4			X			X	X								X	X	X	X
APP.3.6.A5				X	X		X				X							
APP.3.6.A6						X	X					X						X
APP.3.6.A7								X	X	X					X			
APP.3.6.A8		X																
APP.3.6.A9							X								X		X	
APP.3.6.A10				X	X						X							
APP.3.6.A11								X	X	X					X			
APP.3.6.A12		X											X	X				
APP.3.6.A13		X	X															
APP.3.6.A14		X	X			X	X	X	X	X					X			
APP.3.6.A15						X	X		X	X				X				
APP.3.6.A16						X	X					X				X		
APP.3.6.A17						X	X					X			X	X		X

APP.3.6.A1 8						X	X					X						X
APP.3.6.A1 9			X															
APP.3.6.A2 0							X	X	X	X					X		X	
APP.3.6.A2 1			X			X	X					X						
APP.3.6.A2 2	X																	



APP.4.2: SAP ERP System

Description

Introduction

Enterprise resource planning systems from SAP (SAP ERP systems) are used to automate and technically support internal and external business processes. SAP ERP systems typically process confidential information, which means that all the components and data must be appropriately protected.

An SAP ERP system (currently on the market under the product names SAP Business Suite and SAP S/4HANA) consists of various modules that can map the organisational structure of an organisation. The modules of an SAP ERP system include accounting, human resources and logistics. The core components of the SAP ERP system are SAP NetWeaver (application server middleware) and SAP HANA (application server and database). SAP NetWeaver enables clients to connect SAP ABAP and SAP Java applications and control processes throughout the system. SAP HANA can analyse large amounts of data for all business units in real time.

Objective

This module describes the risks to be considered for SAP ERP systems and how these systems can be securely installed, configured and operated. It is aimed at Chief Information Security Officers and administrators who are in charge of planning and implementing SAP ERP systems.

Not in Scope

The module is limited to the core installation of an SAP ERP system and focuses on the specific characteristics of the underlying SAP NetWeaver application server. This module will not describe all the SAP products available in detail. The following descriptions are limited to the configuration of the SAP Basis and do not address the configuration of the modules or applications. Requirements for developing ABAP programs can be found in the module APP.4.6 *SAP ABAP Programming*. Furthermore, no adjoining IT systems, operating systems, databases or similar elements are considered in detail; for these subjects, please refer to specific modules such as SYS1.2.2 *Windows Server 2012*, SYS.1.3 *Unix Server* or APP.4.3 *Relational Database Systems*. Likewise, this module does not deal with SAP HANA. Current product names are deliberately omitted, as these change frequently.

Threat Landscape

For module APP.4.2 *SAP ERP System*, the following specific threats and vulnerabilities are of particular importance:

Lack of Consideration of SAP Security Recommendations

If an SAP ERP system is set up without taking SAP's recommended security guides into account, this can lead to serious security problems in the system. This is the case, for example, if SAP recommendations for user and authorisation management are not implemented correctly. If SAP recommendations for protecting communication or interface operation using RFC and web services are ignored, vulnerabilities can also occur. This can leave the entire system open to attacks.

Missed or Delayed Application of Patches and SAP Security Notes

SAP ERP systems, which consist of different modules and components, are complex systems that usually process sensitive data. SAP therefore regularly publishes patches and security notes to correct software errors and known vulnerabilities. If new patches or SAP security notes are not applied promptly or at all, open vulnerabilities could be exploited by attackers. They could thereby manipulate SAP ERP systems and cause confidential data to be compromised, services to fail or entire business processes to come to a halt.

Lack of Planning, Implementation and Documentation of an SAP Authorisation Concept

The planning and implementation of SAP authorisation concepts is often inadequate or non-existent as a result of the high demands placed on them by the functional and technical complexity of many organisations. However, lack of a well thought-out authorisation concept can often mean that users are assigned more authorisations than necessary. These users could then deliberately manipulate or accidentally damage the SAP ERP system, thus putting its integrity, confidentiality and availability at risk.

In addition, the design of authorisations in S/4HANA systems must be precisely mapped and synchronised between the integrated ABAP, HANA and NetWeaver Gateway components (for Fiori applications); otherwise, contradictory authorisations could be assigned.

If the SAP authorisation concept is not sufficiently documented, assigned authorisations can no longer be traced and maintained. This would make it possible for employees who have already left the organisation or are entrusted with new tasks to still access SAP ERP systems.

Lack of SAP Documentation and Contingency Concepts

If the persons in charge have failed to create or maintain documentation for the SAP ERP system, it will no longer be possible to trace how the SAP ERP system was set up or what its initial settings were. This could delay restoration of service times in an emergency or cause business-critical processes to fail completely. This threat also exists if there are no contingency plans that describe in detail how the persons in charge should proceed in the event of an emergency.

Requirements

The specific requirements of module APP.4.2 *SAP ERP System* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	BCM Officer, Department, Developer, Head of IT

Basic Requirements

For module APP.4.2 *SAP ERP System*, the following requirements **MUST** be implemented as a matter of priority:

APP.4.2.A1 Secure Configuration of the SAP ABAP Stack

The SAP ABAP stack **MUST** be configured securely. For this purpose, the respective profile parameters **MUST** be set, e.g. for password security, authentication and encryption. The system change option and the clients **MUST** also be configured, IMG customising carried out, and the operating system commands saved.

APP.4.2.A2 Secure Configuration of the SAP Java Stack

The SAP Java stack **MUST** be configured securely if it is used. Security mechanisms and concepts that are different from the SAP ABAP stack **MUST** be created for this. Administrators **MUST** therefore know the architecture of the Java stack and how it is administered. In addition, unnecessary services **MUST** be shut down, standard content removed, HTTP services protected, and access to administration interfaces restricted.

APP.4.2.A3 Network Security

To guarantee network security, appropriate concepts **MUST** be created that factor in the SAP ERP system and the settings made in the system.

Furthermore, SAProuter and SAP Web Dispatcher **SHOULD** be used to implement and maintain a secure SAP network.

In order to avoid vulnerabilities due to misinterpretations or misunderstandings, the IT Operation Department, firewall operations, portal operations and SAP operations **MUST** be coordinated.

APP.4.2.A4 Protection of the Standard SAP User IDs Supplied

Immediately after installing an SAP ERP system, the default passwords for standard user IDs **MUST** be changed. Suitable measures **MUST** also be taken to secure the standard SAP user IDs that have been set up. Certain standard user IDs **MUST NOT** be used, e.g. for RFC connections and background jobs.

APP.4.2.A5 Configuration and Protection of SAP User Administration

SAP user administration for ABAP systems **MUST** be undertaken carefully and securely. Activities such as creating, changing and deleting users; resetting and unlocking passwords; and assigning roles and profiles **MUST** be part of the user administration tasks. The user administrator **MUST** be sufficiently trained in SAP user administration and **SHOULD** deepen and update their knowledge regularly.

APP.4.2.A6 Creation and Implementation of a User and Authorisation Concept [Department, Developer, Head of IT]

A user and authorisation concept **MUST** be developed and implemented for SAP ERP systems. The following points **MUST** be considered for this:

- The identity principle, minimum principle, job principle, document principle of accounting, document principle of authorisation administration, segregation of duties principle (SoD), approval principle, standard principle, written form principle and control principle **MUST** be taken into account.
- User, authorisation, and profile administrators **MUST** have separate responsibilities and authorisations.
- Procedures **MUST** be defined within authorisation administration for creating, changing, deleting and transporting roles, as well as for transporting SU24 default values. Authorisation roles **SHOULD** be created and maintained in the development system. They **SHOULD** be transported using the Transport Management System (TMS). Authorisations **SHOULD** be created, saved and assigned to the user in authorisation roles (PFCG roles) in a role-based authorisation concept. Since individual critical actions in the roles cannot always be avoided, they **SHOULD** be covered by mitigation controls.
- In the context of assigning authorisations to users, procedures **MUST** be defined for requesting, approving, changing and deleting authorisations. All authorisations **SHOULD** be assigned in line with the principle of minimum authorisations.
- Naming conventions **MUST** be defined for user IDs and technical role names.
- Default values and check indicators **SHOULD** be maintained in transaction SU24. The procedure **SHOULD** be described in the user and authorisation concept.
- Legal and internal framework conditions, such as the German principles of proper accounting (GoB), the German Commercial Code (HGB) or internal requirements of the organisation, **MUST** be taken into account.

The user and authorisation concept **SHOULD** also cover the operation of technical accounts, including the authorisation of background and interface users.

Appropriate control mechanisms **SHOULD** be applied to monitor the absence of SoD conflicts in roles and the assignment of critical authorisations to users.

If other components such as SAP HANA and SAP NetWeaver Gateway (for Fiori applications) are used in addition to the ABAP back end, the design of the authorisations among the components **MUST** be coordinated and synchronised.

APP.4.2.A7 Protection of SAP Databases

Access to SAP databases **MUST** be secured. Administrators **SHOULD** only be able to access the databases with SAP tools if possible. If third party software is used, additional security measures **MUST** be implemented, e.g. SAPR3 or SAP<SID> users **MUST** not be used to connect to the database. In addition, standard passwords (SAPR3 or SAP<SID>) **MUST** be changed and certain database tables (such as USR* tables) placed under special protection.

APP.4.2.A8 Protection of the SAP RFC Interface

To protect the Remote Function Call (RFC) interface, RFC connections, RFC authorisations and RFC gateways **MUST** be configured securely.

Uniform administrative guidelines **MUST** be created and implemented for all RFC connections. For this purpose, the required RFC connections **SHOULD** be defined and documented. Connections with a stored password **SHOULD** not be configured from lower privileged to higher privileged systems (e.g. from Dev to Prod). RFC connections that are no longer used **MUST** be deleted.

All RFC gateways **MUST** be securely administered and suitable profile parameters **MUST** be set, e.g. gw/monitor, gw/reg_no_conn_info and snc/permit_insecure_start. All connections via a gateway **MUST** be analysed and evaluated in terms of security. Furthermore, logging **MUST** be enabled. Access control lists (ACLs) **MUST** be defined.

APP.4.2.A9 Protection and Monitoring of the Message Server

The message server **MUST** be secured by appropriate settings in the profile parameters. Among other things, it **MUST** be decided whether ACLs are to be set up for the internal message server. The message server **MUST** be monitored using appropriate mechanisms so that, for example, system failures on the message server are detected quickly.

APP.4.2.A10 Regular Implementation of Security Corrections [Department]

Support packages and patches for the SAP ERP system **MUST** be evaluated promptly after publication. A decision **MUST** be made on whether to import each support package or patch. If a support package or patch is not or cannot be imported, the decision and reasons **MUST** be documented. The SAP ERP system **SHOULD** be updated regularly.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module APP.4.2 *SAP ERP System*. They **SHOULD** be implemented as a matter of principle.

APP.4.2.A11 Secure Installation of an SAP ERP System

When installing an SAP ERP system, current SAP security guides and documentation **SHOULD** be taken into account. In addition, the organisation's security policy **SHOULD** be observed. It **SHOULD** also be ensured that the SAP ERP system is installed on a secure operating system.

APP.4.2.A12 SAP Authorisation Development [Department, Developer, Head of IT]

The technical authorisations **SHOULD** be developed on the basis of technical specifications. Furthermore, SAP authorisations **SHOULD** be adapted or newly created on the development system of the SAP landscape. In cases involving S/4HANA, this **SHOULD** also include authorisation development on HANA databases. Repository roles **SHOULD** be set up and transported here. Database privileges **SHOULD NOT** be assigned directly to users.

For software developed in-house (transactions, authorisation objects), transaction SU24 **SHOULD** be maintained (assignments of authorisation objects to transactions). Full authorisation (*) or intervals in object values **SHOULD** be avoided.

Authorisation development **SHOULD** be carried out as part of change management.

It SHOULD be ensured that the production system is adequately protected against authorisation changes and that no developer keys are assigned. The quality assurance system SHOULD be operated in the same way as the production system when assigning authorisations and adding settings.

APP.4.2.A13 SAP Password Security

To ensure secure logins to the SAP ERP system, profile parameters, customising switches, or a security policy SHOULD be configured appropriately.

The hash algorithms used for the stored hash values of the passwords in an SAP ERP system SHOULD comply with the current security standards (see CON.1 *Crypto Concept*). Access to tables with hash values SHOULD be restricted.

APP.4.2.A14 Identification of Critical SAP Authorisations [Department]

The handling of critical authorisations SHOULD be strictly controlled. These authorisations, roles and profiles SHOULD only be assigned restrictively. This SHOULD also be ensured for critical role combinations and additive effects (e.g. cross authorisations).

Critical authorisations SHOULD be regularly identified, reviewed and evaluated. The SAP profiles SAP_ALL and SAP_NEW* and the SAP authorisation object S_DEVELOP (with change authorisations ACTVT 01 and 02) SHOULD not be assigned in the production system. Emergency users SHOULD be excluded from this requirement.

APP.4.2.A15 Secure Configuration of the SAP Router

The SAP router SHOULD regulate the access to the network and complement the existing firewall architecture appropriately. It SHOULD also control access to the SAP ERP system.

APP.4.2.A16 Implementation of Security Requirements for the Windows Operating System

The SAP ERP system SHOULD NOT be installed on a Windows domain controller. The SAP-specific users, such as <sid>adm or SAPService <sid>, SHOULD be secured. After the installation the user <db><sid> SHOULD be locked.

The user SAPService <sid> SHOULD NOT have any interactive login rights. With respect to these authorisations, the system resources associated with the SAP ERP system (such as files, processes and shared memory) SHOULD be protected.

Appropriate settings SHOULD be used to secure the specific authorisations of the Guest, System, SAP system users = <sapsid>adm, SAPService<SAPSID>; Database users = <database-specific users>; and user groups created by the SAP ERP system.

APP.4.2.A17 Implementation of Security Requirements for the Unix Operating System

Access authorisations SHOULD be defined for the SAP ERP system directories in Unix. The passwords of the system-specific users <sid>adm and <db><sid> SHOULD also be changed. After the installation the user <db><sid> SHOULD be locked.

APP.4.2.A18 Deactivation of Unsafe Communication

Communication with and among SAP ERP systems SHOULD be secured with SNC. If the database and the SAP application server are operated on different systems, the database connection SHOULD be encrypted appropriately. The internal services of the SAP application server SHOULD ONLY communicate with each other using TLS.

APP.4.2.A19 Definition of Security Policies for Users

Specific security policies for passwords and login restrictions SHOULD be created for the respective users and user groups. For example, users with critical authorisations SHOULD be protected by strong password rules (SECPOL transaction). The security policies SHOULD be correctly assigned to the users and checked regularly.

APP.4.2.A20 Secure SAP GUI Settings

The SAP GUI SHOULD be installed on all clients and updated regularly. SAP GUI ACLs SHOULD also be activated and appropriate administration rules distributed and activated.

APP.4.2.A21 Configuration of the Security Audit Log

The security audit log (SAL) SHOULD be configured with appropriate filter settings so that security-critical events are logged correctly. Appropriate profile parameters SHOULD also be set for the SAL.

APP.4.2.A22 Protection of the Spool in the SAP ERP System [Developer]

It SHOULD be ensured that data from sequential data processing (spool, print) can only be accessed to a limited extent. Unauthorised users SHOULD also be prevented from accessing the TemSe data store used by the SAP spool system. The authorisations granted SHOULD be checked regularly.

APP.4.2.A23 Protection of SAP Background Processing [Developer]

The SAP background processing SHOULD be protected from unauthorised access. For batch jobs, various system user IDs SHOULD be defined and created according to their functional areas. Dialogue users SHOULD NEVER be authorised for this.

APP.4.2.A24 Activation and Protection of the Internet Communication Framework (ICF)

It SHOULD be ensured that only necessary ICF services are activated. All ICF services that are under an ICF object SHOULD only be activated individually. ICF authorisations SHOULD be assigned restrictively and communication SHOULD be encrypted.

APP.4.2.A25 Secure Configuration of the SAP Web Dispatcher

The SAP Web Dispatcher SHOULD not be the first entry point from the Internet into the SAP ERP system. The SAP Web Dispatcher SHOULD always be up to date. It SHOULD be configured securely.

APP.4.2.A26 Protection of the Customer's Own Code in the SAP ERP System

A custom code management process SHOULD be defined so that the customer's own code is exchanged or removed if it can be replaced by standard SAP code or is no longer used. The requirements from the module APP.4.6 *SAP ABAP Programming* SHOULD also be taken into account.

APP.4.2.A27 Auditing of the SAP ERP System [Department]

To ensure that all internal and external policies and requirements are met, all SAP ERP systems SHOULD be audited regularly. The Security Optimisation Service in SAP Solution Manager SHOULD be used for this. The results of the audit SHOULD be evaluated and documented.

APP.4.2.A28 Creation of a Contingency Concept [BCM Officer]

A contingency concept SHOULD be created and operated for SAP ERP systems. It SHOULD secure the business activities and comply with the requirements of crisis management or business continuity management. The following points SHOULD be described and defined in the contingency concept:

- incident detection and response
- data backup and recovery concept
- business continuity management

The contingency concept SHOULD be updated at regular intervals.

APP.4.2.A29 Setting Up an Emergency User

User IDs SHOULD be created for emergency users. The IDs and authorisations that have been set up SHOULD be strictly controlled and precisely documented. In addition, all activities performed by emergency users SHOULD be logged.

APP.4.2.A30 Implementation of Continuous Monitoring of Security Settings

The accuracy of all the SAP ERP system security settings SHOULD be constantly monitored. The proper application of all patches and updates SHOULD also be monitored. SAP monitoring SHOULD be integrated into the organisation's general system monitoring.

APP.4.2.A31 Configuration of SAP Single Sign-On

If multiple SAP ERP systems exist, users SHOULD access the systems with SAP single sign-on (SAP SSO). The SAP ERP systems that will be included in the SSO mechanism SHOULD be determined in the planning phase. SSO SHOULD be configured and operated securely.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.4.2 *SAP ERP System* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.4.2.A32 Real-Time Recording and Alerting of Irregular Processes (CIA)

The most important security recording functions in SAP ERP systems (security audit log, system log, etc) SHOULD be continuously monitored. An employee in charge SHOULD be automatically alerted in the event of suspicious transactions. To analyse SAP-specific security incidents and differentiate false reports from actual security incidents, employees SHOULD either be trained or third-party services should be used.

Additional Information

For more information about threats and security safeguards for module APP.4.2 *SAP ERP System*, see the following publications, among others:

[BVASJ]	User administration with AS Java: SAP SE, https://help.sap.com/saphelp_nw73/helpdata/de/45/b90177cf2252f8e10000000a1553f7/content.htm?no_cache=true , last accessed on 05.10.2018
[DSAPERP]	SAP ERP 6.0 test guide: Best Practice - Recommendations, German-speaking SAP User Group (DSAG), 2015, https://www.dsag.de/go/leitfaeden , last accessed on 21.03.2018
[SAPAUD]	SAP Audit Management: SAP SE, https://help.sap.com/saphelp_fra110/helpdata/de/ab/ce1b52bd543c3ae10000000a441470/frameset.htm und https://help.sap.com/saphelp_erp60_sp/helpdata/de/f9/558f40f3b19920e10000000a1550b0/content.htm , last accessed on 21.03.2018
[SAPHELP]	SAP Help Portal: SAP SE, https://www.help.sap.com/viewer/index , last accessed on 21.03.2018
[ZVB]	Central User Administration: SAP SE, https://help.sap.com/doc/erp2005_ehp_07/6.07/de-DE/8d/270bea613d2443bad6ce0524f08ca0/frameset.htm , last accessed on 21.03.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.4.2 *SAP ERP System*:

G 0.14 Interception of Information / Espionage

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.14	G 0.21	G 0.22	G 0.23	G 0.25	G 0.28	G 0.30	G 0.31	G 0.32	G 0.39	G 0.43	G 0.45	G 0.46
APP.4.2.A1	X			X	X	X	X	X	X	X	X	X	X
APP.4.2.A2	X			X	X	X	X	X	X	X	X	X	X
APP.4.2.A3	X										X		
APP.4.2.A4	X		X	X	X	X	X	X	X	X	X	X	X
APP.4.2.A5	X		X	X	X	X	X	X	X	X	X	X	X
APP.4.2.A6	X		X	X	X	X	X	X	X	X	X	X	X
APP.4.2.A7	X		X	X	X	X	X	X	X	X	X	X	X
APP.4.2.A8	X		X	X	X	X	X	X	X	X	X	X	X
APP.4.2.A9					X								
APP.4.2.A10						X							
APP.4.2.A11	X			X	X	X	X	X				X	X
APP.4.2.A12	X		X						X				X
APP.4.2.A13				X									
APP.4.2.A14			X				X		X				
APP.4.2.A15	X			X			X						
APP.4.2.A16	X			X			X						
APP.4.2.A17	X			X			X						
APP.4.2.A18	X			X									
APP.4.2.A19				X									
APP.4.2.A20				X									
APP.4.2.A21		X	X	X			X	X	X				

APP.4.2.A22	X		X										X
APP.4.2.A23	X		X										X
APP.4.2.A24				X									
APP.4.2.A25				X									
APP.4.2.A26	X	X	X	X	X	X	X			X	X	X	X
APP.4.2.A27	X		X	X			X	X					
APP.4.2.A28					X								
APP.4.2.A29					X							X	X
APP.4.2.A30	X	X	X	X	X	X	X	X	X		X	X	X
APP.4.2.A31				X									
APP.4.2.A32	X	X	X	X	X	X	X	X	X	X	X	X	X



APP.4.3: Relational Database Systems

Description

Introduction

Database systems (DBS) are widely used in organising, creating, modifying and managing large data collections with the help of computers. A DBS consists of a database management system (DBMS) and one or more databases. A database is a collection of data and corresponding descriptions (metadata) that is stored persistently in the database system. Since database systems are of central importance in an IT infrastructure, there are essential security requirements in this regard. The core processes of an organisation largely depend on information from databases, which results in corresponding availability requirements. Additionally, there often are high requirements regarding the confidentiality and integrity of the information stored in the databases.

Objective

The objective of this module is to demonstrate the secure operation of relational database systems and the appropriate protection of the information processed and stored in databases. It thus describes requirements that can be used to securely plan, implement and operate database systems and reduce specific threats.

Not in Scope

This module describes requirements for relational database systems. Security requirements for non-relational database systems are not part of the present module; they are described in module APP.4.4 *Non-Relational Database Systems*.

In order to continuously protect the information in databases, security requirements regarding the design of the database tables and access to the database should already be taken into account during application development. However, this module does not cover these requirements.

In addition, the module does not cover threats and requirements related to the operating system or hardware on which the database system is based. These aspects are covered in the corresponding operating system-specific modules of the *IT Systems* layer, e.g. SYS.1.3 *Unix Server* or SYS.1.2.2 *Windows Server 2012*.

Threat Landscape

For module APP.4.3 *Relational Databases*, the following specific threats and vulnerabilities are of particular importance:

Insufficient Capacity of System Resources

If the hardware of the database system does not have sufficient system resources, there is the risk of the database failing completely or working improperly. One consequence is that it may not be possible to store data. Moreover, the resources may be utilised heavily during peak times, which may result in a deterioration in performance. In turn, this may cause applications to be executed improperly, or not at all.

Enabled Default User Accounts

Upon initial installation (in a database management system's delivered state), user and administration accounts are frequently not protected at all or only with publicly known passwords. This entails the risk of these accounts being misused. For example, an attacker may use the publicly known login data to log into the database management system as a user or even as an administrator. Afterwards, they may read, manipulate, or delete the configuration or the data stored.

Poor Assignment of Authorisations

If authorisations are assigned or managed incorrectly, persons in charge or users of the database management system may obtain authorisations beyond those that are absolutely necessary. It will thus be possible for the persons in charge or users with too many authorisations to execute prohibited actions on the database management system with far-reaching consequences, as the following example shows:

Due to an incorrect SQL statement (for example, in an installation script), a user accidentally deletes a very large number of datasets from the database. Afterwards, it is determined that the user actually only needed read-only rights with regard to these datasets – not the delete rights that were unnecessarily granted.

Unencrypted Database Connection

In their default configuration, many database management systems establish unencrypted connections to applications. If the communication between the applications and database management system is not encrypted, others may eavesdrop on the data and access information or manipulate it during transmission.

Data Loss in a Database

Due to hardware, software, or human errors, data may be lost in a database. Since important information for applications is stored in databases in most cases, services may be unavailable or entire production processes may come to a halt.

Loss of Integrity of Stored Data

Incorrectly configured databases, software errors or manipulated data may cause an infringement on the integrity of the information contained in a database. If this is only detected at a later point in time or not at all, core processes of the organisation may be strongly impaired.

For example, if the integrity relationships (referential integrity) between the tables are not defined correctly, this may result in the data in the database being in an erroneous condition. If this error is only detected during production operations or not at all, the inconsistent data is not the only thing that will require time-consuming cleansing and reconstruction. The damage that has occurred over time may be extensive – for example, when the data in question is critical. Examples of critical data include tax-relevant data, accounting data or even controlling data for entire production systems.

SQL Injections

SQL injections are a frequently used type of attack on database systems. If an application accesses the data of an SQL database, SQL commands are transmitted to the DBMS. If input data within the application is validated insufficiently, an attacker may import his/her own SQL commands into the application that can then be edited with the authorisation of the application's service account. This way, an attacker may read, manipulate or delete data; add new data; or even call system commands. Although SQL injections primarily refer to applications in the front end, they have significant effects on the database system itself and the related infrastructure.

Insufficient Patch Management

Due to the comprehensive functional scope of database management systems, errors or vulnerabilities occur relatively frequently and **MUST** be corrected by the manufacturer using patches and updates. However, if these are not provided promptly by the manufacturer or their installation is delayed for operational reasons, vulnerabilities can be exploited and the database management system successfully attacked. As a consequence, it may be possible for attackers to manipulate the systems as a means of stealing business-critical data, causing services to fail, or bring entire production processes to a halt.

Insecure Configuration of the Database Management System

Frequently, functions that are not required are enabled in the default configuration of the database management system, which makes it easier for potential attackers to read or manipulate information in the database. For example, an attacker may establish a connection to a programming interface not used by the organisation due to a default installation that was not changed in order to administer the DBMS without having to provide any authentication. As a consequence, they may access the databases of the organisation without being authorised to do so.

Malware and Insecure Database Scripts

In many database management systems, it is possible to automate certain actions. To do this, scripts are executed in the context of the database, for example with the help of the Procedural Language/Structured Query Language (PL/SQL). This also includes so-called database triggers. However, if these are not checked by the process owner before they are used, there is the risk that the database scripts will not meet the software development requirements of the organisation.

An attacker may also manipulate core functions (e.g. data dictionary tables) of a database – for example, with the help of malware or database scripts. Detecting this kind of attack is very hard. Malware and a lack of script quality can endanger the confidentiality, integrity and availability of the data stored in the databases.

Requirements

The specific requirements of module APP.4.3 *Relational Database Systems* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Developer, Process Owner, Head of IT, Supervisor

Basic Requirements

For module APP.4.3 *Relational Database Systems*, the following requirements **MUST** be implemented as a matter of priority:

APP.4.3.A1 Creation of a Security Policy for Database Systems

Based on the general security policy of the organisation, a specific security policy for database systems **MUST** be drawn up that comprehensively describes the requirements and specifications for the secure operation of database systems. The policy **MUST** be known to all employees responsible in the field of database systems and **MUST** be the basis of their work. If the policy is changed or there are deviations from the requirements, this **MUST** be agreed with the CISO and documented. The correct implementation of the policy **MUST** be regularly reviewed. The results **MUST** be documented in an appropriate manner.

APP.4.3.A2 Installation of the Database Management System

It **MUST** be ensured that the installation packages of the database management system come from secure sources. Patches already published **MUST** be installed before operating the DBMS.

APP.4.3.A3 Basic Hardening of the Database Management System

The database management system **MUST** be hardened. For this, a checklist of the steps to be performed **MUST** be compiled and completed. All passwords **MUST** also be changed according to the internal requirements of the organisation. All passwords **MUST** be stored in an encrypted form. The basic hardening **MUST** be reviewed and, if required, adapted at regular intervals.

APP.4.3.A4 Controlled Creation of New Databases

New databases **MUST** be created in accordance with a defined process. If a new database is created, basic information on the database **MUST** be documented in a comprehensible manner.

APP.4.3.A5 User and Access Control Policy

The authorisations for roles, profiles and user groups that are necessary for database management systems **MUST** be added to the organisation's user and access control policy (see ORP.4 *Identity and Access Management*).

A process **MUST** be established to control how database users and their authorisations are created, approved, configured, modified and withdrawn or deleted. In so doing, users **MUST NOT** be granted more access rights than are necessary to perform their respective tasks (“need-to-know” principle). All changes **SHOULD** be documented. The configured users and the authorisations assigned to them **MUST** be reviewed and, if required, adapted at regular intervals.

APP.4.3.A6 Changing Passwords [Process Owner]

All passwords of the database users **MUST** comply with the password policy of the organisation (see *ORP.4 Identity and Access Management*). It **MUST** be ensured that the passwords are changed if there is the slightest suspicion of a related security incident. Particularly regarding privileged database accounts and service accounts, the process of changing passwords **SHOULD** be planned carefully and (if necessary) coordinated with the persons in charge of the application.

APP.4.3.A7 Prompt Installation of Security Updates

Existing security updates for the database management system and the operating system **MUST** be installed promptly. A test system **MUST** be used in advance to ensure that the security updates are compatible and do not cause any errors. Prior to installing a patch, the database system **MUST** be backed up (see *APP.4.3.A9 Backing Up a Database System*).

Additionally, a role **MUST** be defined that will be responsible for regularly obtaining information on known vulnerabilities in the database management system and available security updates. Furthermore, it **MUST** be checked whether the update intervals of the database management system can be adapted to the update cycles of the manufacturer. The results **SHOULD** be documented transparently.

APP.4.3.A8 Database Logging

Security-relevant events on the database system **MUST** be logged with an unambiguous timestamp. In so doing, the type and the extent of logging **MUST** be adapted to the protection needs of the information to be processed. Additionally, it **MUST** be checked whether logging the specialised applications together with the database cover all the information necessary to identify operational and security-relevant changes to the database infrastructure and the applications. Logging **SHOULD** be performed in such a way that the log files cannot be changed retrospectively. More detailed information can be found in *OPS.1.1.5 Logging*.

APP.4.3.A9 Backing Up a Database System

System backups of the DBMS and the data **MUST** be performed at regular intervals. The database system **MUST** also be backed up before a new database is created. For this, the admissible service programs **SHOULD** be used.

All transactions **SHOULD** be backed up in such a way that they can be recovered at any time. If a data backup exceeds the available capacity, an advanced concept (e.g. incremental backups) **SHOULD** be drawn up in order to back up the database. The recovery parameters **SHOULD** be specified based on the protection needs of the data (see *CON.3 Backup Concept*).

Standard Requirements

For module *APP.4.3 Relational Database Systems*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

APP.4.3.A10 Selection of Appropriate Database Management Systems

Prior to procuring database management systems, requirements regarding the DBMS SHOULD be defined and documented in a requirements catalogue. Afterwards, the database management systems being considered SHOULD be evaluated based on the catalogue. The results SHOULD be documented.

APP.4.3.A11 Sufficient Capacity of Hardware [Head of IT, Process Owner]

Database management systems SHOULD be installed on hardware with sufficient capacity. The hardware SHOULD have sufficient reserves in order to meet potentially increasing requirements. If resource bottlenecks become apparent during operations, these SHOULD be eliminated at an early stage. When setting up hardware capacity, the growth expected for the scheduled deployment period SHOULD be taken into account.

APP.4.3.A12 Uniform Configuration Standard for Database Management Systems [Head of IT]

A uniform configuration standard SHOULD be defined for all the database management systems deployed. All database management systems SHOULD be configured and operated in the same manner according to this standard. If an installation requires a deviation from the configuration standard, all steps SHOULD be approved by the CISO and documented transparently. The configuration standard SHOULD be reviewed and adapted as required at regular intervals.

APP.4.3.A13 Restrictive Utilisation of Database Links

It SHOULD be ensured that only persons in charge are authorised to create database links (DB links). If such links are created, private DB links MUST be preferred to public DB links. All DB links created by the persons in charge SHOULD be documented and reviewed at regular intervals. Additionally, DB links SHOULD also be taken into account when the database system is backed up (see APP.4.3.A9 *Backing Up a Database System*).

APP.4.3.A14 Reviewing Database System Backups

The backups performed SHOULD be reviewed at regular intervals to determine whether the integrity of the backup files is still guaranteed. In addition, the employees responsible SHOULD regularly practice recovering databases quickly in the event of an emergency.

APP.4.3.A15 Training of Database Administrators [Supervisor, Head of IT]

It SHOULD be guaranteed that only sufficiently trained employees administer the database management system. A training schedule SHOULD be drawn up to ensure that persons in charge of databases will be trained in good time on matters of information security (see ORP.3 *Awareness and Training*) and performance, as well as on the features of new database management system versions.

APP.4.3.A16 Encryption of Database Connections

The database management system SHOULD be configured in such a way that database communications are always encrypted. The cryptographic methods and protocols used to this end SHOULD comply with the internal specifications of the organisation (see CON.1 *Crypto Concept*).

APP.4.3.A17 Data Transfer or Migration [Process Owner]

If data is transferred to a database initially or on a regular basis, the manner of transfer SHOULD be defined in advance. After data is transferred, checks SHOULD be performed to ensure that it is complete and has not been changed.

APP.4.3.A18 Database Management System Monitoring

Parameters, events and operating conditions of the database management system SHOULD be defined that are critical for secure operations. These SHOULD be monitored using a monitoring system. Threshold values SHOULD be defined for all critical parameters and events. If these values are exceeded, there MUST be an appropriate reaction (e.g. the employees responsible must be informed). Application-specific parameters, events and their threshold values SHOULD be coordinated with the persons in charge of the specialised applications (see also APP.4.3.A11 *Sufficient Capacity of Hardware*).

APP.4.3.A19 Protection Against Malicious Database Scripts [Developer]

If database scripts are developed, binding quality criteria SHOULD be defined in this regard (see CON.8 *Software Development*). Database scripts SHOULD be subjected to comprehensive tests on separate test systems prior to being used productively. The results SHOULD be documented.

APP.4.3.A20 Regular Audits

All components of the database system SHOULD be checked regularly as to whether all the specified security safeguards have been implemented and are configured correctly. In so doing, it SHOULD be checked whether the documented status corresponds to the actual status, whether the configuration of the database management system corresponds to the documented standard configuration, whether all the database scripts are necessary, and whether they meet the organisation's quality standards. Additionally, the log files of the database system and the operating system SHOULD be checked for irregularities (see DER.1 *Detecting Security-Relevant Events*). The audit results SHOULD be documented transparently and compared against the target condition. Deviations SHOULD be investigated.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.4.3 *Relational Database Systems* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.4.3.A21 Use of Database Security Tools (CI)

Information security products SHOULD be used for databases. The products used SHOULD provide the following functions:

- creation of an overview of all database systems
- extended configuration options and rights management of the database
- detection and prevention of possible attacks (e.g. brute force attacks on a user account, SQL injections)

- audit functions (e.g. checking configuration requirements)

APP.4.3.A22 Contingency Planning (CIA)

A business continuity plan SHOULD be drawn up for the database management system to define how emergency operations can be implemented and which resources are necessary in this regard (see DER.4 *Business Continuity Management*). Additionally, the business continuity plan SHOULD define how regular operations can be recovered from emergency operations. The business continuity plan SHOULD define the reporting channels, reaction paths, resources and Process Owner reaction times that are necessary in order to quickly escalate a possible emergency. Based on the recovery coordination plan, all IT systems that depend on the database SHOULD be identified in advance and taken into consideration.

APP.4.3.A23 Archiving (CIA)

If the data of a database system needs to be archived, a corresponding archiving concept SHOULD be drawn up. It SHOULD be ensured that the existing data will be available at a later point in time in a complete and consistent manner.

The archiving concept SHOULD define both archiving intervals and the storage period of the archived data. Additionally, the technology used to archive the database SHOULD be documented. The archived data SHOULD be used for regular recovery tests. The results SHOULD be documented.

APP.4.3.A24 Data Encryption in the Database (C)

The data in the databases SHOULD be encrypted. In so doing, the following factors (among others) SHOULD be considered beforehand:

- effects on performance
- key management processes and methods, including separate key storage and security
- effects on backup recovery concepts
- functional impact on the database (for example, sorting options)

APP.4.3.A25 Security Checks of Database Systems (CIA)

Security checks SHOULD be conducted on database systems at regular intervals. The systemic and manufacturer-specific aspects of the database infrastructure (e.g. directory services) used and the database management system deployed SHOULD be considered within the framework of security checks.

Additional Information

For more information about threats and security safeguards for module APP.4.3 *Relational Database Systems*, see the following publications, among others:

[ACSDSG]	White Paper: Datenbank-Sicherheit – Grundüberlegungen [Database Security – Basic Considerations]: Oracle, January 2016, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/160901_oracle_Datenbank-Sicherheit.pdf , last accessed on 27.09.2018
----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[ACSDVC]	White Paper: Datenbanksicherheit in Virtualisierungs- und Cloud-Computing-Umgebungen [Database Security in Virtualisation and Cloud Computing Environments]: McAfee, October 2013, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/131004_McAfee.pdf ,last accessed on 27.09.2018
[ACSHSD]	White Paper: Die Top 10 der häufigsten Sicherheitsrisiken bei Datenbanken [Top 10 Most Common Database Vulnerabilities: McAfee, December 2017, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/zusatzinfos_angebote/20171219_McAfee_Whitepaper.pdf , last accessed on 27.09.2018
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 15.11.2017
[TELEKOM_DB]	Privacy and Security Assessment Process: Database Systems Security Requirements: Deutsche Telekom, October 2016, https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/sicherheit/privacy-and-security-assessment-verfahren-342724 , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.4.3 *Relational Database Systems*:

- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0.14	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.39	G 0.40	G 0.43	G 0.45	G 0.46
APP.4.3. A1			X								X		X									
APP.4.3. A2					X			X					X									
APP.4.3. A3	X	X		X		X	X	X					X					X				X
APP.4.3. A4	X	X		X		X	X	X					X									X
APP.4.3. A5								X					X		X	X	X					
APP.4.3. A6				X		X	X	X					X			X						
APP.4.3. A7	X			X		X	X	X				X	X					X				X
APP.4.3. A8										X	X						X					
APP.4.3. A9						X	X														X	X
APP.4.3. A10			X		X																	
APP.4.3. A11									X	X	X								X			
APP.4.3. A12	X	X		X		X	X	X					X					X				X
APP.4.3. A13	X						X	X					X									
APP.4.3. A14						X	X														X	X



APP.4.6: SAP ABAP Programming

Description

Introduction

In-house software developments are often programmed in SAP systems. There are many reasons for this: business processes or reporting requirements can be individually adapted to the organisation with the help of in-house developments, or special functions that are not available out-of-the-box can be created.

In-house developments are programmed by developers within the organisation or by commissioned developers. ABAP (Advanced Business Application Programming) is often used for this in the SAP environment.

ABAP is a proprietary, platform-independent programming language from SAP. It was developed for programming commercial applications in the SAP environment, and its basic structure bears a slight resemblance to the COBOL language. Its important features are:

- integration of an authentication, role and authorisation concept
- use of a proprietary, database-independent SQL derivative (Open SQL)
- support of communication between different SAP systems
- integration of audit options

Objective

This module shows ABAP developers and security testers the relevant technical risks that can result from in-house ABAP developments. It also defines requirements that show how ABAP programs can be securely developed and used.

This module requires basic knowledge of ABAP and in-house ABAP development tools.

Not in Scope

This module supplements the modules CON.8 *Software Development*, CON.4 *Selection and Use of Standard Software* and CON.5 *Development and Use of Generic Applications* with specific aspects of developing ABAP programs.

This module is not a complete guide to developing ABAP programs; it describes the general risks of the ABAP programming language and defines requirements for developing ABAP programs from a security point of view.

As web applications only make up a very small proportion of all ABAP applications in SAP implementations, web vulnerabilities are not the focus of this document.

Threat Landscape

For module APP.4.6 *SAP ABAP Programming*, the following specific threats and vulnerabilities are of particular importance:

Lack of Authorisation Checks

In SAP, authorisations are only checked if a corresponding authorisation check has been implemented by the developer in the program. Without a check like this in the program code, no test is carried out to see if the user is actually authorised. For program code developed in-house, (important) authorisation checks are often forgotten. As a result, the entire authorisation concept often becomes ineffective and unauthorised persons can access the data stored in the SAP system. This can also result in compliance requirements being violated, which can have serious consequences – especially for audits.

Loss of Confidentiality or Integrity of Critical Data

SAP systems contain a significant amount of business-critical information. The SAP standard provides for various mechanisms to protect this data. However, incorrect ABAP custom developments could result in unauthorised access to business-critical information and enable employees or attackers to transfer data to an uncontrollable environment. Likewise, critical data can be manipulated with the help of ABAP programs by bypassing the standard SAP security mechanisms.

Injection Vulnerabilities

Injection vulnerabilities relate to an attacker's ability to insert control characters or commands into an application via the input field. A successful attack can disrupt the planned program sequence with unexpected commands.

Injection vulnerabilities represent the greatest security risk for in-house developments. Incorrect code in an ABAP application can sometimes allow an attacker to completely control an SAP system. Since such attacks are very complex and come in many variants, they are very difficult to detect and resolve without special training.

Bypassing Existing SAP Security Mechanisms

The SAP standard provides various protection mechanisms for data. They include client separation, identify management, roles and authorisations. However, these security mechanisms can be deliberately bypassed or unintentionally omitted in the code.

Requirements

The specific requirements of module APP.4.6 *SAP ABAP Programming* are listed below. As a matter of principle, the Head of Development is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is in charge of ensuring that all requirements are met and verified according to the agreed security concept. There can be additional roles with further responsibilities

for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of Development
Further Roles	Developer

Basic Requirements

For module APP.4.6 *SAP ABAP Programming*, the following requirements **MUST** be implemented as a matter of priority:

APP.4.6.A1 Protection of Reports with Authorisation Checks [Developer]

It **MUST** be ensured that only authorised users can start self-programmed evaluations (reports). Therefore, each report **MUST** perform explicit authorisation checks appropriate to the context.

APP.4.6.A2 Formally Correct Evaluation of Authorisation Checks [Developer]

Each authorisation check in the code **MUST** be evaluated by querying the return value SY-SUBRC.

APP.4.6.A3 Authorisation Check Before Starting a Transaction [Developer]

If developers use the CALL TRANSACTION command, a start authorisation check **MUST** always be performed before the command is executed.

APP.4.6.A4 No Proprietary Authorisation Checks [Developer]

Each authorisation check **MUST** be carried out technically using the AUTHORITY-CHECK command provided for this purpose. Proprietary authorisation checks, e.g. based on user names, **MUST NOT** be used.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module APP.4.6 *SAP ABAP Programming*. They **SHOULD** be implemented as a matter of principle.

APP.4.6.A5 Drawing Up a Policy for ABAP Development

A policy **SHOULD** be drawn up for the development of ABAP programs. In addition to naming conventions, the policy **SHOULD** contain specifications for ABAP elements that may or may not be used. The requirements from this module **SHOULD** be included in the policy. The policy **SHOULD** be binding for developers.

APP.4.6.A6 Complete Execution of Authorisation Checks [Developer]

During an authorisation check in ABAP code (AUTHORITY-CHECK <OBJECT>), it **SHOULD** be ensured that all fields are checked for the relevant authorisation object. If individual fields are not actually required, they **SHOULD** be marked as DUMMY. In addition, the exception reason **SHOULD** also be documented in the field.

APP.4.6.A7 Authorisation Check During Input Processing [Developer]

The function codes and screen elements of ABAP Dynpro applications SHOULD be consistent. If a screen element has been deactivated, an application SHOULD NOT react to the events of this element without adequate authorisation checks. If certain entries in a Dynpro menu are hidden or individual buttons are deactivated, the corresponding function codes SHOULD also not be executed.

APP.4.6.A8 Protection Against Unauthorised or Manipulative Access to the File System [Developer].

If access to files on the SAP server depends on user input, this input SHOULD be validated before access.

APP.4.6.A9 Authorisation Check in Remote-Enabled Function Modules [Developer]

It SHOULD be ensured that all remote-enabled function modules in the program code explicitly check whether the initiator is authorised to execute the corresponding business logic.

APP.4.6.A10 Execution of Operating System Commands [Developer]

Each call of a permitted operating system command should be preceded by a corresponding authorisation check (authorisation object S_LOG_COM). User input SHOULD NOT be part of a command. For this reason, operating system calls SHOULD only be executed using standard SAP function modules intended for this purpose.

APP.4.6.A11 Avoiding Planted Malicious Code [Developer]

The ABAP commands INSERT REPORT and GENERATE SUBROUTINE POOL SHOULD NOT be used because they could dynamically create and execute new, potentially harmful ABAP programs at runtime.

APP.4.6.A12 Avoiding Generic Module Execution [Developer]

Transactions, programs, function modules, and methods SHOULD NOT be generically executable. If there are important reasons for a generic execution, where and why this is happening SHOULD be documented in detail. In addition, a whitelist SHOULD be defined that contains all the permitted modules. Before a module is called, the user input SHOULD be compared against the whitelist.

APP.4.6.A13 Avoiding Generic Access to Table Contents [Developer]

Table contents SHOULD not be read generically. If there are important reasons for doing this, where and why this is happening SHOULD be documented in detail. It SHOULD also be ensured that the dynamic table name is restricted to a controllable list of values.

APP.4.6.A14 Avoiding Native SQL Statements [Developer]

The ABAP Database Connectivity (ADBC) interface SHOULD NOT be used. User input SHOULD NOT be part of ADBC commands.

APP.4.6.A15 Avoiding Data Leaks [Developer]

A sufficiently secure authorisation check SHOULD be performed before business-critical data is displayed, transmitted or exported. Planned (intended) export possibilities SHOULD be documented.

APP.4.6.A16 No System-Dependent Execution of Functions [Developer]

ABAP programs SHOULD NOT be programmed in a system-dependent manner – that is, so they can only be executed on a particular SAP system. However, should this be absolutely necessary, it SHOULD be documented in detail. In addition, the code SHOULD then be checked manually.

APP.4.6.A17 No Client-Dependent Execution of Functions [Developer]

ABAP programs SHOULD NOT be programmed in a client-dependent manner – that is, so they can only be executed by a particular client. However, should this be absolutely necessary, it SHOULD be documented in detail. In addition, further security measures SHOULD then be taken, such as a manual code review or quality assurance on the corresponding client.

APP.4.6.A18 Avoiding Open SQL Injection Vulnerabilities [Developer]

Dynamic Open SQL SHOULD not be used. If database access with dynamic SQL conditions is necessary, user input SHOULD NOT be transferred in the respective query. If this is nevertheless the case, the user input MUST be checked (output encoding).

APP.4.6.A19 Protection Against Cross-Site Scripting [Developer]

Custom-developed HTML in Business Server Page (BSP) applications or HTTP handlers SHOULD be avoided as far as possible.

APP.4.6.A20 No Access to Data From Another Client [Developer]

The automatic client separation SHOULD NOT be bypassed. Data from other clients SHOULD NOT be accessed using EXEC SQL or the Open SQL option CLIENT SPECIFIED.

APP.4.6.A21 Ban on Hidden ABAP Source Code [Developer]

The source code of an ABAP program created in-house SHOULD always be readable. Techniques that prevent this (obfuscation) SHOULD NOT be used.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.4.6 *SAP ABAP Programming* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.4.6.A22 Use of ABAP Code Analysis Tools (CIA)

An ABAP code analysis tool SHOULD be used to automatically check ABAP code for security-relevant programming errors, functional and technical errors and quality vulnerabilities.

Additional Information

For more information about threats and security safeguards for module APP.4.6 *SAP ABAP Programming*, see the following publications, among others:

[DSAGABAP]	Best Practice Guidelines for Development: Useful Tips for ABAP Development, German-speaking SAP User Group (DSAG), 2016, https://www.dsag.de/seite/best-practice-
------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

	guide-leitfaden-development-abap-20, last accessed on 05.10.2018
[SABAP]	Sichere ABAP-Programmierung: Wiegenstein, Schumacher, Schinzel, Weidemann, SAP Press 2009

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module *APP.4.6 SAP ABAP Programming*:

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.28 Software Vulnerabilities or Errors

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.14	G 0.16	G 0.19	G 0.22	G 0.28	G 0.39	G 0.45	G 0.46
APP.4.6.A1	X		X	X	X		X	X
APP.4.6.A2	X		X	X	X		X	X
APP.4.6.A3	X		X		X			
APP.4.6.A4	X		X	X	X		X	X
APP.4.6.A5					X			
APP.4.6.A6					X			X
APP.4.6.A7					X			X
APP.4.6.A8	X	X	X	X	X		X	X
APP.4.6.A9	X		X		X			
APP.4.6.A10	X	X	X	X	X	X	X	X
APP.4.6.A11	X		X	X	X	X	X	X
APP.4.6.A12	X		X	X	X		X	X
APP.4.6.A13	X		X	X	X		X	X
APP.4.6.A14	X	X	X	X	X		X	X
APP.4.6.A15	X	X	X		X		X	
APP.4.6.A16	X	X	X	X			X	X
APP.4.6.A17	X	X	X	X			X	X
APP.4.6.A18	X	X	X	X	X		X	X
APP.4.6.A19	X	X	X	X	X	X	X	X
APP.4.6.A20		X	X	X	X		X	X
APP.4.6.A21	X	X	X	X		X	X	X

APP.4.6.A22					X			
-------------	--	--	--	--	---	--	--	--



APP.5.1: General Groupware

Description

Introduction

The term groupware (also called collaborative software) refers to applications and systems that can be used by several persons (groups) to work together over spatial and/or time-related distances. With the help of groupware systems, groups may cooperate and coordinate appointments. Documents and data can be used and edited simultaneously by several users with the help of groupware, which provides for more efficient flows of information.

Among other things, the term "groupware systems" refers to the groupware server, the associated groupware clients and the required groupware services. Along with the basic features (project management, e-mail, calendar, notes, etc), newer applications offer social media extensions that improve employees' communication and cooperation.

Objective

The objective of this module is to protect information that is stored, processed or transmitted in and with groupware. To this end, the IT components used for groupware and their interfaces must be suitably secured and appropriate methods must be established.

Not in Scope

The module only includes specific threats and requirements regarding groupware systems. Threats and requirements regarding the specific modules of server platforms, operating systems, and clients are not part of the module. These can be found in the modules *SYS.1.1 General Server* and *SYS.2.1 General Client*, as well as in the respective operating-system-specific modules.

Within the context of an information domain, the module *APP.5.1 General Groupware* is mostly used in combination with another specific module of layer *APP.5 E-mail/Groupware/Communication*; this must also be implemented separately. Among others, these modules include *APP.5.2 Microsoft Exchange and Outlook* and *APP.5.5 Instant Messaging*.

Threat Landscape

For module *APP.5.1 General Groupware*, the following specific threats and vulnerabilities are of particular importance:

Poor Planning of Groupware

Compliance with the groupware process is not possible without correspondingly documented rules and a defined security process within the organisation. Potential security risks are particularly likely to occur if the groupware has been incorporated improperly into the directory services, databases are deduplicated, and the specific aspects of groupware are not documented in a security policy.

If the process-related, organisational, and technical regulations are neglected when planning groupware systems, the resulting freedoms may cause incorrect settings and programming, or even expose the systems to (internal/external) attacks. This would impair the groupware systems, the groupware process, and cross-process interfaces in fulfilling their tasks.

Incorrect Configuration of Groupware

Since groupware systems are complex, the many possible settings and interdependent parameters involved may cause numerous security issues. For example, server components may be operated on inappropriate systems. Additionally, it may be possible to ignore essential settings (for example, encryption of individual groupware services or limitations of rights in line with authorisation management). These security gaps may cause a significant loss of availability, authenticity and confidentiality of information and thereby impair the functions of the groupware systems and the integrity of processed data.

If rights are assigned incorrectly for a groupware database, this may cause damaging data leak scenarios or unapproved manipulations in the authorisation management of the organisation. These manipulations could result in incorrect settings that impair the entire groupware system or individual services, for example.

Misuse of Macros Developed In-House and Programming Interfaces for Groupware Services

Many tools and applications have programming interfaces (APIs, for example) for providing other applications with certain features or extending the application's range of functions. However, groupware may be misused to spread malware. This includes, for example, malware that infects groupware systems directly in order to obtain, change or delete information.

Macros may also be used to forward or relocate messages, dates or tasks. If macros are incorrect or incorrect values are calculated by them, index errors, for example, may cause incorrect results and possibly lead the organisation to take poor business decisions.

Incorrect Assignment of Site and Data Access Rights for Groupware Services

If site access rights to a groupware client or access rights regarding stored data in groupware services are not limited to the necessary extent, security gaps may arise. Operations can also be impaired if these rights are created and administered improperly and employees are not able to access information they require, for example. It may also be possible for attackers to access confidential information and view sensitive data as a result.

Insufficient Administrator Knowledge of Groupware Systems

Even minor configuration errors may impair the security of a groupware system. Personnel with poor knowledge of groupware applications and services may cause security gaps accidentally due to the complex system architectures and specific protection mechanisms of the groupware used. An insufficiently trained administrator will also not be able to react effectively

in case of an emergency (e.g. in the event of malfunctions and compromised systems). Administrators with insufficient training and awareness may cause undesired conditions within the groupware services and processes. This can include end devices and groupware systems that are not fully synchronised, or time zones leading to incorrect start times for existing appointments on the calendar.

Data Loss in Groupware Applications

The loss of stored data in groupware applications may have serious effects on business processes, and thus on an entire organisation. If data associated with groupware applications is falsified or lost, the very existence of commercial organisations may be threatened. In government agencies, the loss or falsification of such data may delay internal administration and business processes (or make it impossible to conduct them at all).

Along with the resulting unproductive time and the cost of recovery, the loss of stored data in groupware applications may lead to long-term consequences such as a loss of trust with customers and partners and a negative public image.

Attacks on Groupware Systems and Applications

Groupware systems and individual groupware applications may be compromised by third parties. In the case of groupware systems, the users, the internal network, the groupware servers used, and the message recipient may be targeted by attacks, for example. Possible security gaps may be used by attackers in order to read, change or delete information in closed groupware systems. If access to the groupware applications is not sufficiently protected, attackers might also access confidential data, for example.

Unreliability of Groupware

Groupware services may be used as a quick and convenient means of exchanging data. However, this is not always reliable: messages can be lost due to faulty IT systems or disrupted transmission paths. The reasons for this include damaged lines, failed network coupling elements or improperly configured communication software. E-mails may also be lost because the recipient's address was specified incorrectly. It may also be possible for third parties to intercept messages or eavesdrop on conversations in a targeted manner.

In their default settings, most groupware services are not secured from a cryptographic point of view. This means that unauthorised persons may be able to view the schedule of groups or individual persons using calendar services.

Requirements

The specific requirements of module APP.5.1 *General Groupware* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible that all requirements are met and verified according to the security concept agreed upon.

Module Owner	IT Operation Department
---------------------	-------------------------

Further Roles	Chief Information Security Officer (ISO), BCM Officer, Data Protection Officer, Head of Organisation, User, Head of IT, Supervisor
----------------------	------------------------------------------------------------------------------------------------------------------------------------

Basic Requirements

For module APP.5.1 *General Groupware*, the following requirements **MUST** be implemented as a matter of priority:

APP.5.1.A1 Secure Installation of Groupware Systems [Head of IT]

All the components necessary for a groupware system (e.g. the security gateways) **MUST** be installed and configured securely according to the planned system landscape. While the system is being installed, all the passwords selected **MUST** be secure. Components that are not used **MUST** be disabled. Furthermore, the installation sources **MUST** be protected against unauthorised access.

APP.5.1.A2 Secure Configuration of Groupware Clients [Head of IT, User]

The groupware clients of the users **MUST** be pre-configured by the administrator in such a way that a maximum level of security can be achieved without any further action by the users. The users **MUST** be made aware of the fact that the configuration may not be changed without corresponding authorisation. Moreover, storing passwords in plain text **MUST** be prevented and forbidden. If messages are stored on a mail server and accessed via the Internet Message Access Protocol (IMAP), a size restriction **MUST** be configured for the server-side mailbox. Prior to executing file attachments, they **MUST** be examined for malware using a protection program. The settings selected for e-mails in HTML format, the preview feature, the e-mail filter rules, and the automatic forwarding of e-mails **MUST** be secure.

APP.5.1.A3 Secure Operation of Groupware Systems [Head of IT, Chief Information Security Officer (CISO)]

All security-relevant service packs, updates and patches for the respective software product **MUST** be installed. Therefore, administrators **MUST** regularly inform themselves about newly discovered vulnerabilities of the groupware systems and the operating systems used and close them promptly. In order to secure groupware systems within an organisation, protection mechanisms against denial-of-service (DoS) attacks **MUST** be implemented. The local communication **MUST** be protected adequately. Communications over public networks **MUST** be encrypted. Furthermore, the access rights **MUST** be restricted to the locally connected users. A policy **SHOULD** be drawn up that includes information on the protocols and services allowed in the respective groupware. In particular, the mail server **MUST** be configured such that it cannot be misused as a spam relay.

APP.5.1.A4 Backup Archiving for Groupware [Data Protection Officer, User, Chief Information Security Officer (CISO)]

In a groupware system, the data **MUST** be backed up at regular intervals. To this end, the manner **MUST** be specified in which the e-mails sent and received by the e-mail clients and e-mail servers are to be backed up. Furthermore, a documented approach **SHOULD** be drawn up as to how e-mails must be archived. In so doing, basic rules **SHOULD** be defined as to how, when and where sent and received e-mails are to be archived – for example, whether this should be performed centrally or locally by the users themselves. Time-related and organisational secur-

ity aspects (for instance) SHOULD be considered when archiving e-mails. The required period SHOULD be reviewed, the process of archiving SHOULD be planned, and a method of recovering e-mails SHOULD be considered.

Standard Requirements

For module APP.5.1 *General Groupware*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

APP.5.1.A5 Definition of Communication Partners [Head of Organisation, Head of IT, Data Protection Officer, Chief Information Security Officer (CISO)]

The types of information specific users may receive SHOULD be specified. If information is to be transferred to a communication partner outside of a user's own organisation, it SHOULD be ensured that the recipient has the necessary authorisations to process this information. All information SHOULD be classified according to its strategic importance for the organisation. Communication partners SHOULD be made aware of the fact that the data transferred may only be used for the purpose for which it was passed on. For data protection reasons (Federal Data Protection Act (BDSG), Transfer Control), a list of persons authorised to receive information – in particular, personal data – SHOULD be drawn up. When transferring data, the communication partners who have received information and those who will in the future SHOULD be clear.

APP.5.1.A6 Substitute Arrangements for E-mail [Supervisor, User, Chief Information Security Officer (CISO)]

For e-mail processing, each employee SHOULD have one appropriate substitute at all times. Substitutes SHOULD be able to access the mailbox of the person they substitute. Alternatively, the e-mails SHOULD be forwarded to the substitute. If e-mails are forwarded, the substituted users SHOULD at least be informed. In order to support processes related to substitute arrangements, specific rules SHOULD be established for the autoreply functions in e-mail programs that can be used to securely control these functions. When employees use the autoreply functions, internal information SHOULD NOT be forwarded.

APP.5.1.A7 Planning the Secure Use of Groupware Systems [Head of IT, Chief Information Security Officer (CISO)]

Prior to introducing a groupware system in an organisation, decisions SHOULD be taken as to what it will be used for and which information clusters are to be processed on the groupware system in the future. A decision SHOULD be taken as to whether a proprietary groupware server is to be used in the organisation or a provider is to be used. The manner in which the groupware clients will access the servers SHOULD also be determined. Separate planning SHOULD be performed for each groupware function to be used, and each function's security aspects should be taken into account in the process.

The planning SHOULD also define which data may be transferred under which framework conditions using groupware services and how this will affect the protection needs in question. A description of how proper file transfers can be guaranteed, e.g. by means of organisational rules or technical safeguards, SHOULD also be created. Furthermore, it SHOULD also be specified whether (and if so, how) group services may be used for private purposes. Organisations SHOULD also specify how employees are to use webmail.

APP.5.1.A8 Defining a Security Policy for Groupware [Head of IT, User, Chief Information Security Officer (CISO)]

A security policy for groupware systems and applications SHOULD be drawn up and updated at regular intervals. All users and administrators SHOULD be informed of new or changed security specifications for groupware systems. The groupware security policy SHOULD comply with the applicable generic security policies of the organisation. It SHOULD be checked whether the security policies are being implemented properly.

There SHOULD be one security policy for users and one for administrators. The policy for the users SHOULD specify how communications can be secured (e.g. for network or e-mail communications), which user access rights are available (e.g. to groupware servers or databases), how information is to be forwarded to communication partners and how transferred information can be secured (e.g. signatures/encryptions). The content to be specified for administrators SHOULD also include the configuration options of the groupware components, the specifications for possible access attempts from other servers to a groupware server and information on the authorised access point from which a groupware server may be accessed.

APP.5.1.A9 Secure Administration of Groupware Systems [Head of IT]

Administrative access and related tasks SHOULD be kept separate based on the responsibilities at hand. To ensure smooth groupware operations, administrators SHOULD be appointed and trained. All administrative tasks in the field of groupware and the authorisations assigned SHOULD be documented sufficiently. Administrators SHOULD only be assigned the authorisations required for their respective tasks. After all groupware components are installed, they SHOULD be configured securely. It SHOULD be ensured that the groupware systems used are dimensioned sufficiently. Trustworthy groupware documentation SHOULD also be taken into account during administration. Regular checks SHOULD be carried out to determine whether the existing documentation is up to date.

APP.5.1.A10 Administrator Training on System Architecture and Groupware System Security [Head of IT, Chief Information Security Officer (CISO)]

In order to properly and securely administer a groupware system, the administrators responsible SHOULD be trained. A schedule SHOULD be considered for the training measures required. The administrators SHOULD be trained in all security-relevant areas of the groupware system. The training SHOULD also focus on:

- an overview of solutions for communication security (e.g. encryption, VPN)
- logging
- securing and administering configuration data
- backups
- incident handling
- disaster recovery measures

APP.5.1.A11 Authorisation Management for Groupware Systems [Head of IT, Chief Information Security Officer (CISO)]

The authorisations assigned – particularly those ones with certain privileges – SHOULD be regularly compared against the authorisation concept and adapted promptly as soon as the tasks of users and administrators have changed. An authorisation concept covering all groupware components SHOULD be drawn up. Authorisations SHOULD be assigned as restrictively as possible. Administrative tasks at the operating system level and the groupware application level SHOULD be kept as separate as possible. Roles and responsibilities within administration SHOULD be separated, as well.

APP.5.1.A12 User Training on Security Mechanisms of Groupware Clients [Head of IT, Chief Information Security Officer (CISO)]

All users SHOULD receive training and instructions regarding their work with the groupware client. In the process, the users SHOULD learn which security mechanisms are available and how these may be used. Those who use groupware SHOULD be made aware of the threats and security safeguards to be observed. The users SHOULD be instructed on potential misbehaviour. They SHOULD also be instructed not to participate in e-mail chain letters or subscribe to a large number of mailing lists.

APP.5.1.A13 Data Verification Prior to Transmission and Elimination of Residual Information [Head of IT, User]

Before a file is transmitted via e-mail using a groupware service, it SHOULD be checked for residual information that may not be published. Users SHOULD be made aware of the risks of residual and additional information in files. In order to minimise these risks, files SHOULD be checked randomly for residual information. Any additional information (properties) of files in standard software formats SHOULD be identified, checked and adapted as required before it is forwarded. It SHOULD also be ensured that files do not include any so-called slack bytes.

APP.5.1.A14 Avoiding Problematic File Formats [User]

It SHOULD be specified how e-mails in HTML format, other file formats and file attachments are to be handled. For e-mails formatted in HTML, a policy SHOULD be created that addresses the relevant content of user training, forwarding settings, conversion options (e.g. to text formats), user instructions and secure and separate workstations that may be available.

APP.5.1.A15 Logging of Groupware Systems [Head of IT]

All security-relevant events on groupware systems SHOULD be logged. To this end, an appropriate logging concept SHOULD be drawn up. Access to the logged data SHOULD be restricted. Important system events such as changes, errors and faults in hardware, operating systems, drivers, services and other software SHOULD be logged and evaluated at regular intervals.

APP.5.1.A16 Handling Spam [Head of IT, User, Chief Information Security Officer (CISO)]

As a matter of principle, all users SHOULD ignore and delete spam e-mails. Spam e-mails SHOULD NOT be replied to, links in the e-mails should not be clicked and attachments should not be executed. If the organisation wants to introduce e-mail filter programs, this SHOULD be coordinated with the Data Protection Officer, the Employee Representatives and the users. Rules SHOULD be established for newsgroups and mailing lists.

APP.5.1.A17 Selecting a Groupware or E-mail Provider [Supervisor, Data Protection Officer]

If an organisation commissions a service provider to operate its groupware server instead of running its own, the functional aspects should be identified and coordinated with the provider. It SHOULD also be ensured that the groupware or e-mail provider will implement all the necessary security mechanisms and operate its servers securely. Necessary internal requirements SHOULD be documented in writing in consideration of the relevant legal aspects. All employees SHOULD be informed of what must be considered when using external groupware services.

APP.5.1.A18 Spam and Virus Protection Using an E-Mail Scanner on the Mail Server [Chief Information Security Officer (CISO)]

An e-mail scanner with an integrated, memory-resistant anti-virus program SHOULD be installed on the central mail server to examine incoming and outgoing e-mails – and their attachments in particular – for spam features and malicious content. Since encrypted e-mails may not be examined automatically, the procedure for such e-mails SHOULD also be defined. If an e-mail scanner is used, all employees, the Data Protection Officer and the Employee Representatives SHOULD be informed.

APP.5.1.A19 Encryption of Groupware [Head of IT, User, Chief Information Security Officer (CISO)]

Data transmitted with the help of groupware systems SHOULD be secured by means of appropriate protection mechanisms. Hence, encryption methods and digital signatures SHOULD be used to guarantee the integrity and confidentiality of electronically transmitted information – for example, with the help of a TLS-encrypted connection.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.5.1 *General Groupware* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account **IN THE EVENT OF INCREASED PROTECTION NEEDS**. Final specification is performed within a risk analysis. The letters in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.5.1.A20 Creating a Business Continuity Plan for Potential Groupware System Failure [BCM Officer, Head of IT, Chief Information Security Officer (CISO)] (A)

A concept specifying how the consequences may be minimised and what is to be done in the event of a failure SHOULD be drawn up. Contingency planning for the groupware system used SHOULD take into account the existing business continuity plan of the organisation. Important tasks in maintaining the groupware system or bringing it back online SHOULD be described in a way that will enable personnel with corresponding training to perform them. A restoration of service plan for the groupware system SHOULD be drawn up that describes how the systems must be restarted in a controlled manner after a failure. Emergency drills for system recovery that also consider all the aspects of a system failing or being compromised SHOULD be performed regularly.

APP.5.1.A21 End-to-End Encryption (CI)

In order to maintain the confidentiality of sensitive information across all communication partners, end-to-end encryption SHOULD be used. Only protocols that correspond to the current state of the art SHOULD be used for encryption (see CON.1 *Crypto Concept*).

Additional Information

For more information about threats and security safeguards for module APP.5.1 *General Groupware*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[KOLAB]	Kolab Groupware: https://docs.kolab.org/ , last accessed on 05.10.2018
[TN170645]	Exchange Server 2016: Microsoft TechNet, https://technet.microsoft.com/de-de/library/mt170645(v=exch.160).aspx , last accessed on 05.10.2018
[ZIMBRA]	Zimbra Groupware: Synacor, https://www.zimbra.com/documentation/ , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.5.1 *General Groupware*:

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation of Hardware or Software

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.40 Denial of Service

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0. 11	G 0. 14	G 0. 15	G 0. 16	G 0. 18	G 0. 19	G 0. 20	G 0. 21	G 0. 22	G 0. 25	G 0. 26	G 0. 27	G 0. 28	G 0. 30	G 0. 31	G 0. 32	G 0. 33	G 0. 36	G 0. 37	G 0. 40	G 0. 41	G 0. 42	G 0. 45	G 0. 46
APP.5.1. A1			X				X		X				X	X	X									
APP.5.1. A2			X				X	X				X		X	X									
APP.5.1. A3					X															X			X	X
APP.5.1. A4				X					X	X													X	
APP.5.1. A5						X													X					X
APP.5.1. A6		X			X	X											X							X
APP.5.1. A7	X				X																			
APP.5.1. A8					X																			
APP.5.1. A9			X	X								X		X	X	X		X	X					
APP.5.1. A10					X		X												X					
APP.5.1. A11		X		X		X										X		X	X					
APP.5.1. A12					X		X												X					
APP.5.1. A13					X	X	X												X					



APP.5.2: Microsoft Exchange and Outlook

Description

Introduction

Microsoft Exchange is a groupware solution for medium-sized to large organisations. It can be used to electronically transmit messages and is equipped with additional services for supporting workflows and managing mobile devices by means of Microsoft Exchange ActiveSync. Microsoft Exchange can be used to manage, deliver, filter and send messages such as e-mails. Microsoft Exchange can also offer and manage typical groupware applications such as newsgroups, calendars and task lists, as well as Unified Messaging. In order to be able to use the features of Microsoft Exchange, client software is necessary in addition to the server service. The combination of Microsoft Exchange servers and Outlook clients is referred to here as the "Microsoft Exchange system".

Microsoft Outlook is a client that is made directly available by installing the Office package from Microsoft or by integrating it into the operating systems of mobile devices. Furthermore, the Outlook Web App makes it possible to access e-mails, contacts and the calendar via a browser, for example. This service is already included in the Microsoft Exchange package.

Objective

The objective of this module is to provide information on typical threats to Microsoft Exchange and Outlook and show how Microsoft Exchange and Outlook can be used securely in organisations.

Not in Scope

The module includes specific threats and requirements regarding Microsoft Exchange systems. Threats and requirements regarding the specific modules of server platforms, operating systems, and clients are not part of the module. These can be found in the modules *SYS.1.1 General Server* and *SYS.2.1 General Client*, as well as in the respective operating-system-specific modules.

The requirements from module *APP.5.1 General Groupware* must be always be fulfilled, as well. The present module specifies and complements the requirements specific to Microsoft Exchange systems.

Threat Landscape

For module APP.5.2 *Microsoft Exchange and Outlook*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Rules for Microsoft Exchange and Outlook

Comprehensive rules and specifications for Microsoft Exchange and Outlook are necessary in order to ensure the security of the information processed using Microsoft Exchange and Outlook. For example, data may be lost, changed or deleted accidentally if Microsoft Exchange is incorporated into Active Directory in an incorrect and uncontrolled manner. The situation is similar if mailbox databases are depublished in an unregulated manner and Microsoft Exchange is not sufficiently considered in the security policy. The same holds true when the Microsoft Outlook clients can access the Microsoft Exchange servers without any controls.

Incorrect Migration of Microsoft Exchange

In practice, Microsoft Exchange systems are more frequently migrated than installed anew. In order to migrate to a new version of Microsoft Exchange Server, it is in some cases necessary to update the operating system to a later version. New operating systems often include requirements regarding the existing domain concept and the existing directory services.

If a migration is not planned and performed carefully, internal communications using Microsoft Exchange may be disrupted dramatically, which might cause a reduction in productivity. During migration, there might be problems regarding the configuration (e.g. due to changed configuration settings for the different versions) or when connecting to directory services. Furthermore, incorrect protocol settings may cause abnormalities regarding information transfer, authentication and encryption.

Inadmissible Browser Access to Microsoft Exchange

Microsoft Exchange allows users to access their own e-mail accounts via a browser. This involves the use of the Internet Information Services (IIS), which are an integral part of Microsoft Exchange Server. If this functionality is planned poorly and configured improperly, it may allow uncontrolled access to the internal network from the outside.

Allowing browsers to access e-mails from the Internet poses very significant risks. Despite not having direct access to the organisation's network, attackers may access e-mails and (for example) view e-mail addresses and content, misuse e-mail features, send spam e-mails, and gain access to internal information of the organisation.

Unauthorised Connection of Other Systems to Microsoft Exchange

Microsoft Exchange systems are tightly intertwined with the Microsoft Windows operating system and only cooperate with third-party systems by means of so-called connectors. With the help of the connectors, other systems may use certain protocols (e.g. POP3) in order to retrieve e-mails from Microsoft Exchange servers.

If the connectors are not taken into consideration when migrating Microsoft Exchange, the existing connectors may be incompatible with the migrated version of Microsoft Exchange. As a consequence, e-mails may be lost or changed accidentally.

Outside of the homogeneous Microsoft environment, security settings not referring to the Microsoft Exchange system are invalid. The same holds true for defined security parameters in Microsoft Exchange that reference Windows Server. If different sub-systems are administered separately, inconsistencies may occur at any time. Improperly connected third-party systems may also cause data to be lost or the system to be blocked.

Improper Administration of Site and Data Access Rights in Microsoft Exchange and Outlook

If access rights to a Microsoft Outlook client and to data stored within Microsoft Exchange and Outlook are created and administered improperly, security gaps may arise. For example, this is the case if rights exceeding those actually necessary are assigned, enabling unauthorised persons to access confidential information.

Incorrect Configuration of Microsoft Exchange

Successful attacks on services such as Microsoft Exchange are frequently made possible by incorrectly configured systems. Since a Microsoft Exchange system is very complex, diverse configuration settings and interdependent parameters may cause numerous security issues. The possible incorrect configurations range from the installation and operation of the Microsoft Exchange components on inappropriate systems, the absence of encryptions and insufficient access restrictions on Microsoft Exchange servers to the incorrect assignment of rights when creating or initialising a Microsoft Exchange database.

Improper Configuration of Outlook

The e-mail client Microsoft Outlook is an important part of the Microsoft Exchange system. Regarding the overall security of the system, it is important that the client be properly configured. The communication protocol selected may already entail specific security issues. Private keys that are used to encrypt and sign e-mails may also be compromised. If network-level encryption is used (based on IPSec or TLS, for example), the encryption mechanism may become ineffective due to an incorrectly configured client. Incorrect configurations may cause security issues such as a loss of confidentiality due to unauthorised access.

Malfunction and Misuse of In-House Macros and Programming Interfaces in Microsoft Outlook

Many software manufacturers equip their tools and applications with programming interfaces (such as APIs). These allow certain functions to be used from other programs or extend the application's own range of functions. Microsoft Outlook may be misused to spread malware. The malware variants include malicious tools and macros that directly exploit Microsoft Outlook and the related e-mail features in order to obtain, change or delete information. Macros can also be used to forward or relocate messages, dates or tasks. Errors in macros may constitute an increased risk in this regard. Index errors in macros may produce incorrect results that cause an organisation to take poor business decisions. Specific consequences may include unnecessary costs or automated data leaks.

Requirements

The specific requirements of module APP.5.2 *Microsoft Exchange and Outlook* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibil-

ities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO), BCM Officer, Head of IT

Basic Requirements

For module APP.5.2 *Microsoft Exchange and Outlook*, the following requirements **MUST** be implemented as a matter of priority:

APP.5.2.A1 Planning the Use of Microsoft Exchange and Outlook [Chief Information Security Officer (CISO), Head of IT] (I)

Before Microsoft Exchange and Outlook are implemented, their use **MUST** be planned carefully. In doing so, the following items **MUST** be taken into account at minimum:

- design of the e-mail infrastructure
- clients or server systems to be connected
- use of functional extensions
- protection of the access ports of the server/client components
- confidentiality, integrity and availability
- protocols to be used
- integration of the server and client systems into their designated network segments

APP.5.2.A2 Selecting an Appropriate Microsoft Exchange Infrastructure [Head of IT]

Decisions **MUST** be taken as to the systems and application components with which the Microsoft Exchange infrastructure is to be implemented and what hierarchy is to be established. When selecting an infrastructure, it **MUST** also be decided whether the systems are to be operated in the cloud or as a local service.

APP.5.2.A3 Authorisation Management

For the systems of the Microsoft Exchange infrastructure, an authorisation concept **MUST** be drawn up, documented appropriately and used. The privileged users and the administrators **MUST** only be assigned the number of authorisations that are necessary to fulfil their tasks (minimum principle). Whether the rights assigned are still appropriate **MUST** be reviewed at regular intervals.

APP.5.2.A4 Access Rights to Microsoft Exchange Objects

The access rights to Microsoft Exchange objects **MUST** be defined on the basis of the least-privilege principle. Server-side user profiles for computer-independent access to Microsoft Exchange data **MUST** be used. The default NTFS authorisations for the Microsoft Exchange dir-

ectory **MUST** be adapted so that only authorised administrators and system accounts are allowed to access the data in this directory.

APP.5.2.A5 Backing Up Microsoft Exchange [BCM Officer]

The existing Microsoft Exchange system **MUST** be backed up prior to any installations and configuration changes, as well as at cyclical intervals.

Standard Requirements

For module APP.5.2 *Microsoft Exchange and Outlook*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

APP.5.2.A6 Secure Installation of a Microsoft Exchange System

The installation **SHOULD** be performed based on a usage plan for Microsoft Exchange and Outlook and the defined security policy (see APP.5.2.A1 *Planning the Use of Microsoft Exchange and Outlook*). Since Microsoft Exchange systems are a highly integral part of the Windows environment (and of Active Directory in particular), the specific corresponding security policies **SHOULD** be taken into consideration. The systems on which Microsoft Exchange and Outlook are to be installed **SHOULD** be secured appropriately.

APP.5.2.A7 Migration of Microsoft Exchange Systems

All migration steps **SHOULD** be planned and documented carefully. The Microsoft Windows system administrators **SHOULD** be involved in the planning phase. The migration planning **SHOULD** consider mailboxes, objects, security policies, Active Directory concepts, e-mail systems and any functional differences in the various versions of Microsoft Exchange and Outlook. The new system **SHOULD** be tested in a separate testing network prior to being installed in order to counteract software errors and compatibility issues.

APP.5.2.A8 Secure Operation of Microsoft Exchange

All infrastructure systems and applications **SHOULD** be configured such that the protection needs are adequately satisfied. To this end, an appropriate basic configuration **SHOULD** be established and documented. The settings of the individual connectors **SHOULD** also be adapted.

The persons in charge **SHOULD** remedy vulnerabilities that have become known promptly depending on the protection needs and the criticality. As a matter of principle, it **SHOULD** be ensured that patches and updates are only obtained from trustworthy sources.

APP.5.2.A9 Secure Configuration of Microsoft Exchange Servers

Microsoft Exchange servers **SHOULD** be configured on the basis of the specifications included in the security concept. A maximum admissible size **SHOULD** be set both for incoming and outgoing messages. Existing connectors **SHOULD** be configured appropriately. Logging of the Microsoft Exchange system **SHOULD** be enabled. A corresponding concept **SHOULD** be created for existing customising.

When using functional extensions (e.g. Microsoft Exchange ActiveSync, port mirroring, spam filters, the Outlook Web App, or data loss prevention), it **SHOULD** be ensured that the requirements defined for the security objectives pertaining to confidentiality, integrity and availability continue to be met.

APP.5.2.A10 Outlook Settings

Only administrators SHOULD be able to change the Outlook environment. For this, a separate Outlook profile with user-specific settings SHOULD be created for every user. The users SHOULD only be able to change select settings (e.g. signature configuration, enabling the autoreply feature) in a user-defined manner. As a matter of principle, it SHOULD NOT be possible to open e-mail attachments automatically. Preview windows and automatic previews SHOULD be disabled. E-mails SHOULD NOT be forwarded automatically.

APP.5.2.A11 Protection of Communications from and to Microsoft Exchange Systems

The protection mechanisms used to secure communications from and to Microsoft Exchange systems SHOULD be decided upon in a comprehensible manner. A decision SHOULD be taken and documented plausibly regarding which of the different possible methods – Internet Protocol Security (IPSec) or Transport Layer Security (TLS) – is to be used.

The following SHOULD be encrypted:

- administration interfaces
- client-server communications
- existing interfaces for web-based distributed authoring and versioning (WebDAV)
- server-to-server communications and message communications
- the public key infrastructure based on the e-mail encryption of Microsoft Outlook (S/MIME)

APP.5.2.A12 Use of Microsoft Exchange for Outlook Anywhere

Outlook Anywhere SHOULD be configured according to the security requirements of the organisation. Access to Microsoft Exchange over the Internet SHOULD be restricted to the necessary users. Communications with Outlook Anywhere SHOULD be encrypted (see APP.5.2.A11 *Protection of Communications from and to Microsoft Exchange Systems*).

APP.5.2.A13 Administrator Training [Head of IT]

Only appropriate and trained personnel SHOULD be assigned to operate the components of the Microsoft Exchange infrastructure.

APP.5.2.A14 User Training on Outlook Security Mechanisms [Chief Information Security Officer (CISO)]

Outlook users SHOULD be trained and made aware of new and existing risks with regard to working with Microsoft Outlook on a regular basis. All users SHOULD be familiarised with relevant security mechanisms and the corresponding procedures within Outlook. This SHOULD also include rules for access mechanisms, forms of authentication and cryptographic specifications for e-mail encryption.

APP.5.2.A15 Application Documentation for Microsoft Exchange

The content of the operating manual for Microsoft Exchange SHOULD be documented plausibly. The operating manual SHOULD describe the phases of commissioning, operation, disposal and restoration of service based on the lifecycle at hand. The documentation SHOULD be protected against unauthorised access. Changes SHOULD be documented or referenced plausibly.

APP.5.2.A16 Drawing Up a Business Continuity Plan for Potential Failures of Microsoft Exchange and Outlook [BCM Officer]

Within the framework of contingency planning, a concept SHOULD be drawn up that can be used to minimise the consequences of a failure of the Microsoft Exchange and Outlook components. The business continuity plan SHOULD define what is to be done in the event of a failure in order to ensure that normal operations will be promptly recovered.

Requirements in Case of Increased Protection Needs

Generic suggestions for module APP.5.2 *Microsoft Exchange and Outlook* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

APP.5.2.A17 Encryption of Microsoft Exchange system databases (CIA)

A concept SHOULD be drawn up for encrypting PST files and information store files. The users SHOULD be informed about the method of operation and the protection mechanisms involved in encrypting PST files. Additional aspects for local PST files that SHOULD be taken into consideration when encrypting Microsoft Exchange system databases include:

- proprietary encryption functions
- degrees of encryption
- mechanisms for securing the data in a PST file

Mechanisms such as the Encrypting File System or Windows BitLocker drive encryption SHOULD be used to secure the data in a PST file.

APP.5.2.A18 Regular Security Checks for Microsoft Exchange Systems (CIA)

The Microsoft Exchange system SHOULD be checked for incorrect configurations and vulnerabilities at regular intervals. To this end, it SHOULD be subjected to a security check performed by different persons at regular intervals. It is advisable to draw up a checklist in this regard in order to guarantee a defined scope. The following aspects SHOULD be taken into consideration during testing:

- regular research on security-relevant information
- authorisations for audit users
- regular examination of authorisations
- examination of whether updates are current
- examination of the security of communication interfaces

The Microsoft Exchange authorisations SHOULD be examined regularly through random testing (at minimum).

Additional Information

For more information about threats and security safeguards for module APP.5.2 *Microsoft Exchange and Outlook*, see the following publications, among others:

[MSTN]	Microsoft Technet: https://technet.microsoft.com/de-de , last accessed on 06.09.2018
--------	----------------------------------------------------------------------------------------------------------------------------------------

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module APP.5.2 *Microsoft Exchange and Outlook*:

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.40 Denial of Service

G 0.45 Data Loss

Elementary Threats Requirements	G 0.15	G 0.16	G 0.18	G 0.19	G 0.21	G 0.22	G 0.25	G 0.26	G 0.28	G 0.30	G 0.31	G 0.32	G 0.36	G 0.40	G 0.45
APP.5.2.A1			X	X		X								X	
APP.5.2.A2			X		X		X	X							
APP.5.2.A3										X	X	X	X		
APP.5.2.A4						X				X		X			
APP.5.2.A5				X											X
APP.5.2.A6					X					X					
APP.5.2.A7			X				X	X							
APP.5.2.A8								X	X						
APP.5.2.A9						X			X						
APP.5.2.A10					X				X	X	X	X			
APP.5.2.A11	X			X		X									
APP.5.2.A12	X			X		X							X		
APP.5.2.A13										X	X				
APP.5.2.A14										X	X				
APP.5.2.A15			X				X	X							
APP.5.2.A16							X	X						X	
APP.5.2.A17				X						X					
APP.5.2.A18					X			X							



SYS.1.1: General Server

Description

Introduction

This module covers general security requirements for all IT systems which make services available to other IT systems, such as clients or other servers. These services can be basic services for the local or external network, but also those that allow the exchange of e-mails or make databases and printer services available. Servers play a key role in information technology, and thus in the well-functioning workflows of an organisation. Servers often perform tasks without users making direct, interactive use of them. In addition, there are server services which directly interact with users and are not perceived as a server service at first glance – for example, X Server in Unix.

Objective

The objective of this module is to protect information which is processed, offered or transmitted by servers, as well as the associated services.

Not in Scope

Server systems are usually operated in operating systems for which specific security requirements must be taken into consideration in each case. For widely used server operating systems, separate modules that complement this module with more specific information can be found in the IT-Grundschutz compendium. The module SYS.1.1 *General Server* forms the basis for the specific modules that are built on it. If a specific module exists for a given system, that module must be used in addition to module SYS.1.1 *General Server*. If there is no specific module for the server systems used, the requirements of this module must be elaborated in a suitable manner.

The respective specific services offered by the server are not part of this module. For these server services, other modules will need to be implemented in addition to this module. These modules are selected based on the results of the IT-Grundschutz modelling process. If interactive usage is also provided for a server system in a particular case (e.g. for a terminal server), the related security aspects related must also be considered separately – for example, by applying the corresponding specified modules.

Threat Landscape

For module SYS.1.1 *General Server*, the following specific threats and vulnerabilities are of particular importance:

Software Vulnerabilities or Errors

The more complex the software, the more frequently programming or design errors occur. Software vulnerabilities are understood to be unintentional programming errors that are not yet known to the user and constitute a security risk to the IT system. New vulnerabilities are always being found in both widely used and brand-new software.

If software errors are not detected and eliminated promptly, the errors resulting from the use of the software may have serious consequences. In the case of common standard software, software vulnerabilities may rapidly result in serious security problems for organisations of all kinds.

Errors in server services can have particularly serious effects. In the case of a vulnerability or an error in a network service, local access rights will not be required to exploit it. An attacker often only needs access via the network. If the server offers a service with a vulnerability or error over the Internet, this error or vulnerability could be exploited by any IT system in the world.

Data Loss

For servers in particular, the loss of data may seriously affect business processes, and the entire organisation as a result. A large number of IT systems, such as clients or other servers, often depend on the availability of the data that is centrally stored there.

When business information of any type is destroyed or corrupted, this can cause delays in business processes and specialised tasks, or even prevent their execution. Overall, the loss of stored data may lead to failures and additional costs for the recovery of the data, and especially to long-term consequences (e.g. a loss of trust among customers and partners, legal consequences, or a negative public image). In many organisations, there are regulations that require that data be stored centrally on servers rather than on local clients. In such cases, the loss of this data will have serious effects; the direct and indirect damage caused may even threaten the existence of an organisation.

Denial of Service

A type of attack referred to as a “denial-of-service” attack seeks to prevent users from using functions or devices that are normally available to them. This type of attack is often connected to the use of distributed resources: the attacker places such high demands on these resources that other users are prevented from carrying out their work and can no longer access resources on which they depend. IT systems are usually also strongly dependent on one another, which means that a shortage of resources on one server can quickly affect others. For example, a shortage of CPU time, memory space or bandwidth may be produced artificially to make it impossible to use a service or resource at all.

Provision of Unnecessary Operating System Components and Applications

When installing the server operating system, it is possible to install all the applications and services supplied. Software which is tested briefly, but no longer needed afterwards is often installed during operations, as well. Those involved are frequently unaware that these unused applications and services are available on the servers. As a result, numerous unused applications and services may be placing an unnecessary load on the server.

These unused applications and services may contain vulnerabilities. If the applications are then no longer updated, they may be an entry point for attackers. If the applications and services in-

stalled are not known, the IT Operation Department will not be aware of the fact that they must also be updated.

Server Overload

If servers do not have sufficient capacity, there will come a point when they no longer meet the requirements of the users. Depending on the type of the affected systems, this may have a large number of negative consequences – for example, the servers or services may be temporarily unavailable or data may be lost. In the case of complex IT landscapes, one overloaded server can result in problems or failures on other servers.

Information systems may be overloaded by

- installed services or applications being configured incorrectly and taking up unnecessary memory as a result
- available disk capacity being exceeded
- a system's processors being used excessively by numerous simultaneous queries
- services requiring too much computing power
- a large number of messages being sent at the same time

Requirements

The specific requirements of module SYS.1.1 *General Server* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Building Services

Basic Requirements

For module SYS.1.1 *General Server*, the following requirements **MUST** be implemented as a matter of priority:

SYS.1.1.A1 Appropriate Installation [Building Services]

Servers **MUST** be operated at locations that may only be accessed by authorised persons. Servers **MUST** therefore be set up and installed in data centres, computer rooms, or lockable server rooms (see the corresponding modules). It **MUST** be regulated who is granted access to the rooms or physical access to the servers themselves. Servers **MUST NOT** be used as personal computers. It **MUST** be ensured that only dedicated removable storage devices and other devices can be connected to the servers.

Adequate spatial separation of the systems to be secured from the systems securing them (e.g. backup servers in different fire zones) **MUST** be ensured to limit the effects of physical damage.

SYS.1.1.A2 User Authentication

In order to use the server, the users **MUST** be authenticated by the IT system. If the users and administrators have to use passwords, secure passwords **MUST** be used. A password policy **SHOULD** be in place. These passwords **MUST** be sufficiently complex, kept secret and changed at regular intervals.

SYS.1.1.A3 Restrictive Granting of Access Rights

Access rights to files stored on the servers **MUST** be granted restrictively. Every user **MAY ONLY** be granted the access rights to files actually required to fulfil their tasks. The access right itself **MUST** be limited to the type of access required. For example, it is very rarely necessary to grant write privileges to program files.

It **SHOULD** be checked at regular intervals whether the authorisations (for system directories and files in particular) correspond to the specifications of the security policy. If possible, only system administrators **SHOULD** have access to system files. The group of administrators with the authorisations required to access these files **SHOULD** be kept as small as possible. Directories **SHOULD** also provide no more than the required privileges for users.

SYS.1.1.A4 Segregation of Duties

It **MUST** be ensured that IDs with administrator rights are only used for administration tasks. For all administrators, additional user IDs **MUST** be configured which have only the restricted rights the administrators need to perform tasks other than administration. Administrators **MUST** use only these user IDs for non-administrative activities. No additional user IDs other than those that are actually required **SHOULD** be created on the server.

SYS.1.1.A5 Protection of Administration Interfaces

Depending on the type of access used (local, remote or central system management), suitable security precautions **MUST** be taken. The methods used for administration **MUST** be defined in the security policy. Administration **MUST** be performed in accordance with the security policy.

Authentication methods adequate for the protection needs of the servers **MUST** be used when users and services log into the system. This **SHOULD** be taken into account for administrative access in particular. Central, network-based authentication services **SHOULD** be used whenever possible.

Administration **MUST** be performed using secure protocols. The alternative possibility of setting up a separate administration network **SHOULD** be considered.

SYS.1.1.A6 Deactivation of Unnecessary Services and IDs

All unnecessary services and applications (especially network services) **MUST** be deactivated or uninstalled from servers. All unused functions in the firmware **MUST** be disabled, as well. User accounts that are not required **MUST** either be deleted or at least disabled in such a way that these IDs cannot be used for logging into the system. Existing default IDs **MUST** be changed or deactivated whenever possible. Preset passwords of default IDs **MUST** be changed. On servers, the disk space for both individual users and applications **SHOULD** be restricted appropriately.

The decisions made SHOULD be documented in such a way that it can be understood which configuration and software equipment was chosen for the servers.

SYS.1.1.A7 Updates and Patches for Firmware, Operating Systems and Applications

Administrators MUST inform themselves regularly about vulnerabilities which become known in the firmware, operating systems, applications and services used. The vulnerabilities identified MUST be eliminated as quickly as possible so that they cannot be exploited by attackers. It MUST be ensured in general that patches and updates are only obtained from trustworthy sources.

When no corresponding patches are available, other suitable safeguards to protect the system MUST be implemented depending on the severity of the vulnerabilities and basic threats.

SYS.1.1.A8 Regular Backups

Backups MUST be performed prior to installations and extensive configuration changes, as well as at defined intervals. These backups MUST make it possible to recover the data stored on the server. In virtual environments, it SHOULD be checked whether the system can be backed up by means of snapshot mechanisms of the virtualisation environment under certain circumstances.

SYS.1.1.A9 Use of Anti-Virus Programs

Depending on the operating system installed, the service provided and other existing protection mechanisms of the server, it MUST be checked whether virus protection programs can and should be used. Concrete statements on whether virus protection is required can usually be found in the operating-system-specific modules of the IT-Grundschutz Compendium. The corresponding signatures of a virus protection program MUST be updated at regular intervals. In addition to real-time and on-demand scans, it MUST also be possible to scan compromised and encrypted data for malware with the solution chosen.

SYS.1.1.A10 Logging

It MUST be decided which minimum information is to be logged by the servers, how long the logged data is to be kept and who is allowed to view the logged data under which conditions. Data protection requirements MUST be taken into consideration. As a matter of principle, all security-relevant system events MUST be logged. At minimum, these include:

- system starts and reboots
- successful and failed login attempts (operating system and application software)
- failed authorisation checks
- blocked data flows (violations of ACLs or firewall rules)
- creation of or changes to users, groups and authorisations
- security-relevant error messages (e.g. hardware defects, exceeded capacity limits)
- warnings of security systems (e.g. virus protection)

Standard Requirements

For module SYS.1.1 *General Server*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.1.1.A11 Defining a Security Policy for Servers

On the basis of the general security policy of the organisation, the requirements for servers SHOULD be specified. The policy SHOULD be known to all administrators and other persons involved in the procurement and operation of the servers, and it must form the foundation of their work. The implementation of the contents required in the policy SHOULD be checked at regular intervals and the results SHOULD be documented in a reasonable manner.

SYS.1.1.A12 Planning the Use of Servers

Every server system SHOULD be planned adequately by taking into account the following aspects at minimum:

- selection of the hardware platform, operating system and application software
- capacity of the hardware (performance, memory, bandwidth, ...)
- type and number of communication interfaces
- power consumption, thermal load, space requirements and design
- realisation of administrative access (see SYS.1.1.A5 *Protection of Administrative Interfaces*)
- user access attempts
- realisation of logging (see SYS.1.1.A10 *Logging*)
- realisation of system updates (see SYS.1.1.A7 *Updates and Patches for Operating Systems and Applications*)
- integration into system and network management, backups and protection systems (virus protection, IDS and similar aspects)

All decisions made in the planning phase SHOULD be documented in such a way that they can be understood at any given future point in time.

SYS.1.1.A13 Procurement of Servers

Prior to procuring one or more servers, a requirements list SHOULD be drawn up that can be used to evaluate the products available on the market.

SYS.1.1.A14 Drawing Up a User and Administration Concept

Procedures, framework conditions and requirements for administrative tasks, as well as the segregation of duties between the different roles of the IT system users, SHOULD be established in a user and administration concept.

SYS.1.1.A15 Uninterruptible and Stable Power Supply [Building Services]

Every server SHOULD be connected to an uninterruptible power supply (UPS). The UPS SHOULD be dimensioned sufficiently in terms of its output power and backup time. If changes have been made to the consumers, it SHOULD be checked again whether the backup time is sufficient. Overvoltage protection SHOULD be available for both the UPS devices and the servers.

The actual capacity of the battery (that is, the backup time the UPS can provide) SHOULD be tested at regular intervals. The UPS SHOULD be maintained at regular intervals. The UPS SHOULD be integrated into the existing system and network management.

SYS.1.1.A16 Secure Installation and Basic Configuration of Servers

Servers SHOULD be installed in such a way that only the required services are selected during installation. Installations on a server SHOULD only be performed by authorised persons (administrators or service providers bound by contract) according to a defined installation process. System and application software SHOULD be obtained from trustworthy installation sources. For repeat installations, suitable installation templates SHOULD be created and used.

All installation steps SHOULD be documented in such a way that the installation can be understood and repeated by a qualified third party based on the documentation.

The basic settings of servers SHOULD be checked and, where necessary, adapted to the specifications of the security policy. The server SHOULD be connected to the Internet only after the installation and configuration have been completed.

SYS.1.1.A17 Approval for Use

Before the server system is connected to a production network and put into production use, it SHOULD be approved. This SHOULD be documented in a suitable manner. Before being approved for use, the installation and configuration documentation and the functionality of the system SHOULD be tested. This SHOULD be performed by a department authorised for this purpose in the organisation.

SYS.1.1.A18 Encryption of Communication Links

For all network services offered and used by the server, it SHOULD be checked whether encryption of the communication links is possible and feasible at a reasonable expenditure. If this is possible at a reasonable expenditure, encryption SHOULD be enabled.

SYS.1.1.A19 Configuring Local Packet Filters

Based on a set of rules, existing local packet filters SHOULD be designed to limit incoming and outgoing communications to the necessary communication partners, communication protocols, ports and interfaces.

SYS.1.1.A20 Restricting Access via Networks

As a matter of principle, the entire network of the organisation SHOULD be protected against unauthorised access by means of a corresponding security gateway. Servers offering external services SHOULD be set up in a demilitarised zone (DMZ).

Servers SHOULD preferably not be positioned in the same IP sub-network as the clients. Servers SHOULD be separated from the clients by at least one router.

SYS.1.1.A21 Operational Documentation

Operational tasks that are carried out on a server SHOULD be clearly documented in terms of what has been done when and by whom. In particular, the documentation SHOULD make configuration changes transparent. Security-relevant tasks (who is authorised, for example, to install new hard disks) SHOULD be documented. Everything that can be documented automatically SHOULD be documented automatically. The documentation SHOULD be protected against unauthorised access and loss.

SYS.1.1.A22 Integration into Contingency Planning

The server SHOULD be taken into account in the business continuity management process. To this end, the contingency requirements for the system SHOULD be determined and appropriate contingency procedures implemented – for example, by drawing up recovery plans or securely storing passwords and cryptographic keys.

SYS.1.1.A23 System Monitoring

The server system SHOULD be integrated into a suitable system monitoring concept which continuously monitors the system status, the functionality of the system and the services operated on it while also reporting error conditions and defined limits which have been exceeded to the operating personnel.

SYS.1.1.A24 Security Checks

Server systems SHOULD be subjected to regular security tests to check their compliance with the security specifications and identify possible vulnerabilities. This SHOULD apply in particular to systems with external interfaces. Given the possibility of indirect attacks via infected systems in the organisation's own network, however, internal server systems SHOULD also be checked accordingly at defined cycles. It SHOULD be examined whether the security checks can also be realised automatically (e.g. by means of suitable scripts).

SYS.1.1.A25 Controlled Decommissioning of a Server

When decommissioning a server, it SHOULD be ensured that no important data that might still be present on the storage media is lost and that no sensitive data remains. There SHOULD be an overview of the data stored in each location on the server. Furthermore, it SHOULD be ensured that services offered by the server will be taken over by another servers when necessary.

A checklist which can be completed when decommissioning a server SHOULD be created. This checklist SHOULD at least include aspects related to backing up data, migrating services and subsequently deleting all data in a secure manner.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.1.1 General Server are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.1.1.A26 Multi-Factor Authentication (C)

In case of high protection needs, secure two-factor or multi-factor authentication for access to the server SHOULD be set up (e.g. with cryptographic certificates, chip cards or tokens). It is

crucial that all administrative access to the server SHOULD be secured by means of multi-factor authentication.

SYS.1.1.A27 Host-Based Attack Detection (IA)

Using host-based attack detection systems (also known as host-based intrusion detection systems, IDS, or intrusion prevention systems, IPS), the system behaviour SHOULD be monitored for abnormalities and misuse. The IDS/IPS mechanisms used SHOULD be appropriately selected, configured and thoroughly tested. If an attack has been detected, the operating personnel SHOULD be alerted in an appropriate manner.

Using operating system mechanisms or suitable additional products, changes made to system files and configuration settings SHOULD be checked, restricted and reported.

SYS.1.1.A28 Redundancy (A)

Server systems with high availability requirements SHOULD be protected adequately against failures. To achieve this, suitable redundancies SHOULD be available at minimum or maintenance contracts SHOULD be concluded with the suppliers. It SHOULD be checked whether high-availability architectures with automatic failover (across various sites, if necessary) are required in case of very high requirements.

SYS.1.1.A29 Setting Up a Testing Environment (CIA)

To be able to test changes to the system or configuration without jeopardising production operations, corresponding test systems SHOULD be available or provided when necessary (e.g. as virtual images). The test systems SHOULD correspond to the production systems (software versions, configuration). For application systems, suitable test data which does not include confidential or personal production data SHOULD be generated.

SYS.1.1.A30 One Service per Server (CIA)

Depending on the threat landscape and the protection needs of the services, only one service SHOULD be operated on each server.

SYS.1.1.A31 Application Whitelisting (CI)

In case of high protection needs, it SHOULD be ensured by means of application whitelisting that only the programs allowed are executed. On the one hand, complete paths and directories SHOULD be defined from which this may be possible. On the other hand, individual applications SHOULD explicitly be allowed to be executed as an alternative.

SYS.1.1.A32 Additional Protection of Privileged Login Information (CI)

The passwords of the administrative accounts SHOULD be separated into several parts and SHOULD also be protected by the dual control principle. Administrative accounts SHOULD be configured so that they will be locked after a previously defined number of incorrect login attempts.

SYS.1.1.A33 Active Administration of Root Certificates (CI)

As part of the procurement and installation of the server, the root certificates that are required for operation of the server SHOULD be documented. Only the previously documented root certificates required for operation SHOULD be present on the server. Regular checks SHOULD be made as to whether the existing root certificates still comply with the organisation's requirements. All certificate stores on the IT system SHOULD be included in these checks.

Additional Information

For more information about threats and security safeguards for module SYS.1.1 General Server, see the following publications, among others:

[ISi-Server]	Absicherung eines Servers (ISi-Server) [Securing a Server (ISi-Server)]: Federal Office for Information Security (BSI), September 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi-server_pdf.html , last accessed on 15.11.2017
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 05.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.1.1 General Server:

- G 0.8 Failure or Disruption of the Power Supply
- G 0.9 Failure or Disruption of Communication Networks
- G 0.14 Interception of Information / Espionage
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0.8	G 0.9	G 0.14	G 0.16	G 0.18	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.39	G 0.40	G 0.43	G 0.44	G 0.45	G 0.46
SYS.1.1. A1	X	X		X							X	X									X		
SYS.1.1. A2			X		X				X						X								
SYS.1.1. A3			X		X				X						X		X						X
SYS.1.1. A4			X		X										X		X						X
SYS.1.1. A5			X		X		X	X	X						X		X						X
SYS.1.1. A6			X		X					X					X								
SYS.1.1. A7							X			X		X		X					X				
SYS.1.1. A8																						X	
SYS.1.1. A9								X	X									X	X				
SYS.1.1. A10										X	X	X			X								
SYS.1.1. A11	X	X		X	X		X				X		X	X	X	X					X	X	
SYS.1.1. A12	X	X		X	X						X		X	X	X			X			X		
SYS.1.1. A13					X					X		X		X			X						

SYS.1.1. A30									X	X				X			X						
SYS.1.1. A31						X	X	X	X								X	X					
SYS.1.1. A32														X		X							
SYS.1.1. A33		X			X													X					



SYS.1.2.2: Windows Server 2012

Description

Introduction

In Windows Server 2012, Microsoft launched a server operating system in September 2012 that featured several improvements regarding security when compared to previous Windows versions (particularly Windows Server 2008 R2). From a technical point of view, the new version builds not on the predecessor, but on the code base of the Windows 8 client operating system. With the Windows Server 2012 R2 release from October 2013, the operating system was improved and extended further in order to turn Windows 2012 R2 into the server equivalent to Windows 8.1 on the client side.

This module addresses the process of securing both Windows Server 2012 and Windows Server 2012 R2; relevant differences and particularities are stated appropriately in each case. In so doing, the term “Windows Server 2012 (R2)” is used when referring to both versions. In both cases, the expiration dates for mainstream and extended support (“end of life”, EoL) are 9 January 2018 and 10 January 2023, respectively.

Objective

The objective of this module is to protect information and processes that are processed and controlled on the basis of Windows Server 2012 (R2).

Not in Scope

The module SYS.1.2.2 *Windows Server 2012* must be applied to all target objects operated in the Microsoft Windows Server 2012 (R2) operating system. It specifies and complements the aspects addressed in module SYS.1.1 *General Server* with the specifics of Windows Server 2012 (R2) without repeating the requirements of module APP.2.2 *Active Directory*.

Within the framework of this module, a default integration into an Active Directory domain is assumed, as is common in companies and public authorities. The particularities of stand-alone systems are only mentioned selectively where the differences appear to be particularly relevant.

The security requirements of possible server roles and functions, such as file servers (APP.3.3 *File Servers*), web servers (APP.3.2 *Web Servers*) or Microsoft Exchange and Outlook (APP.5.2 *Microsoft Exchange and Outlook*), are covered in separate modules, as is the subject of virtualisation (SYS.1.5 *Virtualisation*). This module is about using built-in resources to achieve basic security at the operating system level regardless of the server's intended purpose.

Threat Landscape

For module SYS.1.2.2 *Windows Server 2012*, the following specific threats and vulnerabilities are of particular importance:

Poor Planning of Windows Server 2012 (R2)

Windows Server 2012 (R2) is a complex, state-of-the-art operating system that offers a large number of functions and configuration options. One example includes the variety of powerful server roles that can be installed. Every additional function increases the number of possible attacks and the likelihood of vulnerabilities and incorrect configurations. There are also a great many degrees of freedom regarding integration into the domain and networking with other systems and services. Even if state-of-the-art Windows versions include good default settings in many areas, there is no case in which the basic configuration is the most secure. Poor planning may result in numerous attack vectors that may be exploited easily by attackers. Furthermore, if central decisions are not made prior to installation, one starts with an insecure and undefined state that is very difficult to remedy.

Careless Cloud Usage

Windows Server 2012 (R2) offers the use of cloud services at various points without having to install third-party software. For example, this includes Microsoft Azure Online Backup or the online storage of BitLocker recovery keys. While cloud services can offer fundamental advantages, especially in terms of availability, using them carelessly can pose risks in terms of confidentiality and dependency on service providers. Unauthorised third parties – be they attackers or state entities – may gain access to data through cloud services, for example. If a cloud service is configured by the provider, this may have significant effects on one's own business processes.

Improper Administration of Windows Servers

Compared to previous versions, many new security-relevant features were added to Windows Server 2012 and Windows Server 2012 R2. In other features, parameters, default configurations and parts of functions were changed. If the administrators have not been trained sufficiently regarding the particularities of the systems, configuration errors and misbehaviour may occur that affect both security and functionality.

Non-uniform Windows Server security settings are a particular risk (e.g. for SMB, RPC, or LDAP). If the configuration is not planned, documented, reviewed and tracked in a centralised and systematic manner, a configuration drift may occur: this means that the more the specific configurations of systems that are similar from a functional point of view begin to differ for no reason and without any documentation, the more difficult it will be to maintain an overview of the status quo and guarantee security in a holistic and consequent manner.

Improper Use of Group Policies (GPOs)

Group policies (GPOs) are a useful and powerful way to configure many (security) aspects of Windows Server 2012 (R2), particularly in a domain. Given the large number of possible settings, it is easy to accidentally set contradictory or incompatible settings or forget subject areas. A non-systematic approach in this regard will, at minimum, cause operational malfunctions that are sometimes difficult to remedy, or even severe vulnerabilities on the server or connected client systems. In particular, improperly used inheritance rules and filters may result in GPOs not being applied to a system at all.

Loss of Encrypted Data

If data is encrypted (e.g. using BitLocker or the device encryption in Windows Server 2012 (R2)), a complete loss of data may occur if the key is lost and there is no recovery key. In this case, a backup containing encrypted data is of no real use.

Loss of Integrity of Sensitive Information or Processes

Windows Server 2012 (R2) has numerous features that are designed to protect the integrity of information processed by the operating system. Every single one of them may entail vulnerabilities. Furthermore, they are often not configured thoroughly for reasons related to perceived user-friendliness or convenience. Information and processes may thus be falsified by unauthorised employees or external attackers, who are frequently able to cover their tracks in the process. In many cases, malware is also used to remotely manipulate information.

Software Vulnerabilities or Errors

All software includes vulnerabilities, and this is all the more true of complex systems such as Windows Server 2012 (R2). Vulnerabilities in components may enable an attacker to inject or execute malware or misuse features of the system and bypass security mechanisms. For example, this may result in information being manipulated or accessed by the wrong people. Every additional role or feature installed increases the risk of vulnerabilities occurring or being discovered by attackers. Not all vulnerabilities immediately become publicly known, and patches are not immediately available for all known vulnerabilities. Furthermore, these patches must first be installed.

Unauthorised Acquisition or Misuse of Administrator Rights

The practice of providing administrators with separate accounts with standard rights for their regular work is now considered a good approach. Administrators must work with more extensive rights at certain points, however, which gives an attacker the opportunity to interfere and take control of such privileges. The misuse of rights by legitimate administrators is a relevant damage scenario, as well. Since these roles are often very powerful, the effects are typically significant, particularly in cases involving domain administrators. Even without guessing or breaking passwords, attackers may use so-called pass-the-hash methods, for example, to read out and misuse appropriate credentials as a means of moving laterally within the network.

Compromised Remote Access

Windows Server 2012 (R2) has a large number of remote administration options that present general potential for misuse. Remote access involving RDP user sessions, for example, may be available to third parties due to insecure or insecurely used protocols, weak authentication (e.g. weak passwords) or incorrect configuration. As a consequence, the server and the information it houses may be compromised to a critical extent. Additional IT systems connected to the server can often be compromised, as well.

Requirements

The specific requirements of module *SYS.1.2.2 Windows Server 2012* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further re-

sponsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	

Basic Requirements

For module SYS.1.2.2 *Windows Server 2012*, the following requirements **MUST** be implemented as a matter of priority:

SYS.1.2.2.A1 Planning of Windows Server 2012

The use of Windows Server 2012 (R2) **MUST** be planned carefully prior to installation. The hardware requirements **MUST** be checked prior to procurement. A justified and documented decision for an appropriate edition of Windows Server 2012 (R2) **MUST** be taken. The purpose of the server **MUST** be specified in so doing, along with the planned integration into Active Directory. The use of cloud services integrated into the operating system **MUST** be considered and planned as a matter of principle. If they are not required, the configuration of Microsoft accounts on the server **MUST** be blocked.

SYS.1.2.2.A2 Secure Installation of Windows Server 2012

The installation medium **MUST** be procured from a demonstrably reliable source. Server roles, features and functions other than those needed **MUST NOT** be installed. If it is sufficient from a functional scope perspective, the server core variant **MUST** be installed. Otherwise, reasons why the server core variant is not sufficient **MUST** be cited. During installation, the latest patches **MUST** first be applied to the server.

SYS.1.2.2.A3 Secure Administration of Windows Server 2012

Local administration accounts **MUST** have secure and unique passwords. All administrators responsible for the server system **MUST** have been trained in the security-relevant aspects of administering Windows Server 2012 (R2). They **MAY NOT** use administrative rights when these are not absolutely necessary. Browsers on the server **MAY NOT** be used for surfing the Internet.

Standard Requirements

For module SYS.1.2.2 *Windows Server 2012*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

SYS.1.2.2.A4 Secure Configuration of Windows Server 2012

Several essential functions and roles **SHOULD NOT** be performed by a single server. Prior to commissioning, the system **SHOULD** be fundamentally hardened. To this end, function-specific security templates for the entire organisation **SHOULD** be created, maintained and rolled out to the server systems. The settings **SHOULD** be tested initially and in the event of changes prior to commissioning. Internet Explorer **SHOULD** only be used in the enhanced security configuration and the enhanced protected mode on the server.

SYS.1.2.2.A5 Protection Against Malware

Except for IT systems with Windows Server 2012 that are operated as stand-alone devices without any network connection or removable media, an anti-virus protection program SHOULD be installed prior to establishing the first connection to the Internet or removable media. The signatures SHOULD be updated at regular intervals. Furthermore, all hard disks SHOULD be scanned completely at regular intervals. Alarms SHOULD be configured that will alert the responsible administrators when viruses are found.

SYS.1.2.2.A6 Secure Authentication and Authorisation in Windows Server 2012

In Windows Server 2012 R2, all users SHOULD be members of the security group "Protected Users". Accounts for services and computers SHOULD NOT be members of the "Protected Users" group. Service accounts in Windows Server 2012 (R2) SHOULD be members of the "Managed Service Account" group so that the passwords of the services are changed regularly and automatically according to the AD guidelines. The PPL protection of the local security authority (LSA) SHOULD be activated. The use of dynamic access rules for resources SHOULD be preferred.

The administrators of Windows Server 2012 (R2) SHOULD use restricted rights when working on their own clients.

SYS.1.2.2.A7 Security Checks on Windows Server 2012

The security configuration of Windows Server 2012 (R2) SHOULD be checked, documented and enhanced at regular intervals using appropriate tools.

SYS.1.2.2.A8 Protection of System Integrity

Secure boot SHOULD be active. AppLocker SHOULD be enabled and configured as stringently as possible. The effects of changes SHOULD be tested in advance.

SYS.1.2.2.A9 Local Communication Filtering

The local firewall SHOULD be enabled for incoming and outgoing network traffic and configured as stringently as possible. The identity of remote systems and the integrity of corresponding connections SHOULD be protected cryptographically.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.1.2.2 *Windows Server 2012* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.1.2.2.A10 Hard Disk Encryption in Windows Server 2012 (C)

For systems running Windows Server 2012 (R2), the storage media SHOULD be encrypted using BitLocker or another product. This SHOULD also apply to virtual machines containing production data. In case of higher protection needs, the TPM SHOULD not be the only key protection. The recovery password SHOULD be stored in Active Directory or another appropriate and secure location. In case of very high confidentiality or deniability requirements, full-volume encryption SHOULD be performed.

SYS.1.2.2.A11 Attack Detection in Windows Server 2012 (CIA)

Security-relevant events in Windows Server 2012 (R2) SHOULD be collected and analysed at a central location. Encrypted partitions SHOULD be blocked after a defined number of decryption attempts.

SYS.1.2.2.A12 Redundancy and High Availability (A)

The availability requirements that can be implemented or supported with the help of operating system functions such as Distributed File System (DFS), ReFS, failover clusters, network load balancing or NIC teaming (LBFO) SHOULD be reviewed. For branches, BranchCache SHOULD be enabled.

SYS.1.2.2.A13 Strong Authentication in Windows Server 2012 (CI)

A role-based administration model SHOULD be developed and implemented for administering different server functions. For critical services, two-factor authentication SHOULD be implemented.

SYS.1.2.2.A14 Shutting Down Encrypted Servers and Virtual Machines (CI)

In order to protect encrypted data during operations, as well, servers that are not required (including virtual machines) SHOULD always be shut down or put on standby. This SHOULD occur automatically whenever possible. Data encryption SHOULD require an interactive step or at least be documented in the security log.

Additional Information

For more information about threats and security safeguards for module SYS.1.2.2 *Windows Server 2012*, see the following publications, among others:

[ISFSY12]	The Standard of Good Practice for Information Security: Area SY1.2 Server Configuration, Information Security Forum (ISF), June 2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 05.09.2018
[PAYNE]	Windows Event Forwarding for everyone: Microsoft Technet, Blog, Jessica Payne, November 2015, https://blogs.technet.microsoft.com/jepayne/2015/11/23/monitoring-what-matters-windows-event-forwarding-for-everyone-even-if-you-already-have-a-siem/ , last accessed on 24.08.2018
[TN831360]	Secure Windows Server 2012 R2 and Windows Server 2012: Microsoft TechNet, November 2013, https://technet.microsoft.com/en-us/library/hh831360.aspx , last accessed on 24.08.2018
[TN831778]	Security and Protection: Microsoft TechNet, February 2014, https://technet.microsoft.com/en-us/library/hh831778.aspx , last accessed on 24.08.2018
[TN832031]	Secure Windows : For Windows 8/8.1 (also applies largely to Windows Server 2012 / 2012 R2), March 2014, https://technet.microsoft.com/en-us/library/hh832031.aspx , last

	accessed on 24.08.2018
[WINLSA]	Configuring Additional LSA Protection: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection , last accessed on 06.09.2018
[WINSPEX]	Windows Server Guidance to protect against Speculative Execution: https://support.microsoft.com/en-us/help/4072698/windows-server-guidance-to-protect-against-speculative-execution

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.1.2.2 *Windows Server 2012*:

- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.33 Shortage of Personnel
- G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.40 Denial of Service

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G0.1.4	G0.1.5	G0.1.8	G0.1.9	G0.2.0	G0.2.1	G0.2.2	G0.2.3	G0.2.5	G0.2.6	G0.2.7	G0.2.8	G0.2.9	G0.3.0	G0.3.1	G0.3.2	G0.3.3	G0.3.6	G0.3.7	G0.3.8	G0.3.9	G0.4.0	G0.4.1	G0.4.2	G0.4.3	G0.4.4	G0.4.5	G0.4.6	
Re-quire-ments																													
SYS.1.2.2.A1			X								X		X																
SYS.1.2.2.A2	X	X		X	X	X	X	X	X	X		X		X	X	X		X	X	X	X	X		X	X	X	X	X	
SYS.1.2.2.A3	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SYS.1.2.2.A4	X	X		X	X	X	X	X	X		X	X	X	X	X		X	X	X	X	X		X	X	X	X	X	X	
SYS.1.2.2.A5	X	X		X		X	X	X	X	X			X		X		X	X	X	X	X		X	X	X	X	X	X	
SYS.1.2.2.A6	X	X		X		X	X	X			X			X	X	X		X	X	X	X	X	X	X	X	X		X	
SYS.1.2.2.A7	X	X	X	X		X	X	X			X	X		X	X	X		X	X	X	X	X	X		X	X	X	X	
SYS.1.2.2.A8						X	X	X	X	X								X		X								X	
SYS.1.2.2.A9	X	X		X		X	X	X						X	X	X				X	X							X	
SYS.1.2.2.A10	X			X		X	X											X	X	X								X	
SYS.1.2.2.A11	X			X		X	X	X				X		X		X						X	X	X	X	X	X	X	
SYS.1.2.2.A12												X															X		
SYS.1.2.2.A13	X	X		X		X	X	X			X			X	X	X		X	X	X	X	X	X	X	X	X		X	



SYS.1.3: Unix Servers

Description

Introduction

The operating systems Linux or Unix are often used on server systems. Examples of classic Unix systems include the BSD series (FreeBSD, OpenBSD and NetBSD), Solaris and AIX. Linux is not a classic Unix system (the kernel is not based on the initial source code on which the development of the different Unix derivatives is based), but a functional Unix system. This module considers all operating systems of the Unix family, including Linux as a functional Unix system.

Linux is free software that is developed by the open-source community. In addition, there are providers that compile and maintain the various software components for distribution and offer further services. In many cases, the distributions

- Debian
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server and
- Ubuntu Server

are used for Linux servers. Furthermore, there are Linux distributions that are customised for special purposes and devices, such as Endian for firewall systems, OpenMediaVault for NAS systems or OpenWRT for routers.

The services offered on a server are often central, which means they are particularly exposed. That is why Unix servers are not only critical for business processes; they are also frequently the focus of attackers. As a result, the availability and protection of Unix servers is of particular importance.

Objective

The objective of this module is to protect information processed by Unix servers. The requirements of the module address mainly Linux servers, but can be generally adapted to Unix servers. Requirements are formulated on how to configure and operate the operating system independently of the intended purpose of the server.

Not in Scope

The module contains basic requirements for creating and operating Unix servers. It specifies and adds specific features of Unix systems to the aspects included in module *SYS.1.1 General Server*.

If the server is to be hosted by a third party and not managed by the organisation, the requirements of module *OPS. 2.1 Outsourcing for Customers* must also be taken into account. Security requirements of possible server functions such as web servers (*APP.3.2 Web Servers*) or servers for groupware (see *APP.5.1 General Groupware*) are covered in separate modules; they are not addressed in this module. The Unix-specific server services NIS, NFS and SSH, which are also discussed in this module, are an exception. Similarly, the topic of virtualisation is addressed not in this module, but in *SYS.1.5 Virtualisation*.

Threat Landscape

For module *SYS.1.3 Unix Servers*, the following specific threats and vulnerabilities are of particular importance:

Unauthorised Collection of System and User Information

With a variety of UNIX programs, it is possible to capture data on users that is stored in the IT system. This also includes data that can provide information on a user's activity profile. Such information includes information on other logged-in users, as well as technical information on installation and configuration of the operating system.

For example, with a simple program that analyses the information provided by the “who” command at certain intervals, any user can generate a precise utilisation profile for an account. In this way it is possible, for instance, to determine when the system administrator or administrators are absent in order to exploit their absence for unauthorised acts. The program also makes it possible to determine which terminals are approved for privileged access. Other programs with similar potential for abuse are “finger” and “ruser”.

Exploitability of the Script Environment

The use of script languages is very common in Unix operating systems. Scripts are lists of individual commands that are stored in a text file and then opened. Due to the large scope of functions of the script environment, attackers may make extensive use of scripts for their purposes. Moreover, it is very difficult to contain activated script languages.

Dynamic Loading of Jointly Used Libraries

The command line option “LD_PRELOAD” loads the specified library before any other libraries required in an application; its functions are used by the application. An attacker could manipulate the operating system so that malicious functions are executed when using certain applications.

Software Procured from Third-Party Sources

In IT systems similar to Unix, it is not unusual for users to download and compile software on their own instead of installing ready-made software packages. When ready-made software packages are used, they are often not only installed from the existing package sources of the Unix derivative, but procured from third-party sources without any further examination. Each

of these alternative paths of software installation entails additional risks because it is possible that incorrect or incompatible software and malware may be installed.

Requirements

The specific requirements of module SYS.1.3 *Unix Servers* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept defined. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	

Basic Requirements

For module SYS.1.3 *Unix Servers*, the following requirements **MUST** be implemented as a matter of priority:

SYS.1.3.A1 User Authentication in Unix

In order to use the Unix server, the users **MUST** be authenticated by the IT system. Authentication via a network **MUST** be encrypted. If a user account is only allowed to use certain services, it **MUST NOT** be possible to use the user account for other services.

SYS.1.3.A2 Careful Allocation of IDs

Each login name, user ID (UID), and group ID (GID) **MUST** only be used once. Every user **MUST** be a member of at least one group. Every GID mentioned in the `/etc/passwd` file **MUST** be defined in the `/etc/group` file. Every group **SHOULD** only contain the users that are absolutely necessary. For networked systems, it **MUST** be ensured that the allocation of user and group names, UIDs and GIDs within the system landscape is performed in a consistent manner.

SYS.1.3.A3 Automatic Integration of Removable Drives (A)

Removable drives such as USB pen drives or CDs/DVDs **MUST NOT** be integrated automatically.

SYS.1.3.A4 Protection of Applications

“ASLR” and “DEP/NX” **MUST** be activated in the kernel and used by the applications to make it harder to exploit vulnerabilities in applications. Security functions of the kernel and of the standard libraries (such as heap and stack protection) **MUST NOT** be deactivated.

SYS.1.3.A5 Secure Installation of Software Packages

Software packages **MUST ONLY** be installed from trusted sources. The integrity and authenticity of the software packages to be installed **MUST** always be checked. If the software to be installed is to be compiled from source code, this **MAY ONLY** be unpacked, configured and compiled using an unprivileged user account. The software to be installed for this **MUST NOT** be installed in the root file system of the server in an uncontrolled manner.

If the software is compiled from the source text, the selected parameters SHOULD be documented appropriately. Based on this documentation, it SHOULD be possible to compile the source text in a transparent and reproducible manner at any time. All further installation steps SHOULD also be documented so that the configuration can be reproduced quickly in emergencies.

Standard Requirements

For module SYS.1.3 *Unix Servers*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.1.3.A6 Managing Users and Groups

The corresponding management tools SHOULD be used for managing users and groups. The configuration files `/etc/passwd`, `/etc/group` and `/etc/sudoers` SHOULD NOT be edited directly.

SYS.1.3.A8 Encrypted Access via Secure Shell

Only SSH SHOULD be used to create an encrypted and authenticated interactive connection between two IT systems. All other protocols whose functions are covered by Secure Shell SHOULD be deactivated completely.

SYS.1.3.A9 Protecting the Boot Process

When booting, the integrity SHOULD be checked from the (pre-) boot loader to the kernel. The keys used for this SHOULD be checked during the initial configuration. It SHOULD be checked whether Secure Boot can be used as part of the UEFI specification.

SYS.1.3.A10 Preventing Further Intrusion When Vulnerabilities Are Exploited

Services and applications SHOULD be protected with individual security policies (e.g. with AppArmor or SELinux). In addition, chroot environments and LXC or Docker containers SHOULD be taken into account here. It SHOULD be ensured that the standard profiles and rules provided are activated.

SYS.1.3.A11 Use of NFS Security Mechanisms

Only servers intended for this purpose SHOULD share directories with other clients (see also APP.3.3 *File Servers*). Only directories with an imperative need SHOULD be exported via NFS (Network File System). The mountable directories SHOULD be reduced to those required in the files `/etc/exports` and `/etc/dfs/fstab`. The mountable directories SHOULD only be shared with certain IT systems and/or users while taking the defined authorisation structure into account.

SYS.1.3.A12 Use of NIS Security Mechanisms

NIS (Network Information Service) SHOULD only be used in a secure environment. The entry `+:::0:0:::` SHOULD NOT be included in `/etc/passwd`, `/etc/group` or any other security-relevant files. The “ypserv” server process SHOULD respond only to queries made by computers which have been designated in advance.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.1.3 *Unix Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk

analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.1.3.A14 Preventing Unauthorised Collection of System and User Information (C)

Information output for users regarding the operating system and access to protocol and configuration files SHOULD be limited to the required extent. Moreover, sensitive information SHOULD NOT be provided as parameters when commands are issued.

SYS.1.3.A15 Additional Protection of the Boot Process (CIA)

The boot loader and kernel SHOULD be signed by self-controlling key material, and unnecessary key material SHOULD be removed.

SYS.1.3.A16 Additional Prevention of Further Intrusion When Vulnerabilities Are Exploited (CI)

The use of system calls SHOULD be limited to those absolutely necessary, particularly for exposed services and applications. The standard profiles and rules (e.g. of SELinux or AppArmor) SHOULD be checked manually and, if necessary, adapted to the organisation's own security policies. If required, new rules and profiles SHOULD be drawn up.

SYS.1.3.A17 Additional Protection of the Kernel (CI)

Using particularly hardened kernels, suitable protection mechanisms such as memory protection, file system protection and role-based access control (which help prevent the exploitation of vulnerabilities and further intrusion within the operating system) SHOULD be used.

Additional Information

For more information about threats and security safeguards for module SYS.1.3 *Unix Servers*, see the following publications, among others:

[ISi-Server]	Absicherung eines Servers (ISi-Server) [Securing a Server (ISi-Server)]: Federal Office for Information Security (BSI), September 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/isi-server_pdf.html , last accessed on 05.09.2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, Juli 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 05.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.1.3 *Unix Server*:

G 0.14 Interception of Information / Espionage

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.14	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.28	G 0.30	G 0.31	G 0.32	G 0.39	G 0.43	G 0.45	G 0.46
SYS.1.3.A1	X			X	X			X						
SYS.1.3.A2	X			X				X	X	X			X	X
SYS.1.3.A3			X		X			X						
SYS.1.3.A4				X	X		X				X			
SYS.1.3.A5		X					X							
SYS.1.3.A6			X					X	X					
SYS.1.3.A8	X				X							X		
SYS.1.3.A9			X		X			X						
SYS.1.3.A10						X	X				X			
SYS.1.3.A11	X			X						X			X	
SYS.1.3.A12			X					X		X				
SYS.1.3.A14	X							X						X
SYS.1.3.A15						X	X							
SYS.1.3.A16	X			X						X			X	
SYS.1.3.A17	X			X						X			X	



SYS.1.5: Virtualisation

Description

Introduction

When IT systems are virtualised, one or several virtual IT systems are executed on a physical IT system. A physical IT system of this kind is referred to as a virtualisation server. Several virtualisation servers may be consolidated to form a virtual infrastructure. Here, the virtualisation servers themselves and the virtual IT systems operated on them may be jointly administered.

The virtualisation of IT systems provides many advantages for IT operations in an information domain. Cost savings are possible in the fields of hardware procurement, power and air conditioning if the resources of the physical IT systems are used more efficiently. However, virtualisation also poses a challenge in operating the information domain. Since the virtualisation technology used affects different areas and fields of work in an information domain, knowledge and experiences from a wide variety of areas must be combined.

Objective

This module describes how virtualised IT systems can be introduced and operated securely in the information domain.

Not in Scope

This module only addresses the virtualisation of entire IT systems; other technologies partially associated with the term “virtualisation” (application virtualisation with the help of terminal servers, storage virtualisation, containers, etc) are not covered.

In the field of software development, the terms "virtual machine" and "virtual machine monitor" are also used for runtime environments (e.g. Java, Microsoft .NET). Runtime environments like these are not addressed in this module either.

Virtual infrastructures are normally administered using specific management systems. Since these can be used to comprehensively access the virtualisation infrastructure, it is important that they be sufficiently secured. This is applicable to both the server (either physical or virtual) used to execute the management software and the product itself. Details are described in module NET.1.2 *Network Management*.

Virtualisation environments are mostly used together with mass storage devices (NAS or SAN). The connection and protection of these systems are not addressed in this module either (for this, see module SYS.1.8 *Storage Solutions*).

Due to virtualisation, the organisation's networks must be structured differently. This subject is not addressed comprehensively in this module. In this regard, module NET.1.1 *Network Architecture and Design* must be implemented. Network virtualisation is also only touched on in the present module. Security aspects of virtual network components are addressed in module NET.1.4 *Network Virtualisation*.

In order to secure virtual IT systems, the modules of the layer SYS *IT Systems* that are applicable in each case must be used.

Threat Landscape

For module SYS.1.5 *Virtualisation*, the following specific threats and vulnerabilities are of particular importance.

Poor Planning of Virtualisation

A virtualisation server makes it possible to operate virtual IT systems, integrates the systems into the data centre and, in so doing, controls their connection to further infrastructure elements such as networks and storage networks. In the absence of any planning as to how the virtualisation servers must be integrated into the existing infrastructure from a technical and organisational point of view, the responsibilities for different areas might not be clearly defined (e.g. for applications, operating systems and network components). Moreover, the responsibilities of different areas may overlap or there may be no appropriate rights structure for separating administrative access for the different areas.

Poor Configuration of Virtualisation

Virtualisation changes the way servers are provisioned. Resources such as CPUs, RAM, network connections and memory are normally configured centrally using a management system and thus no longer depend on hardware and cabling. As a consequence, configuration errors may arise more quickly. For example, if a virtual IT system with high protection needs is incorrectly located in an external DMZ, the system may be accessed from the Internet and is thereby exposed to increased risk.

Insufficient Resources for Virtual IT Systems

Virtualisation servers require disk space that is provided either locally in the virtualisation server itself or in a storage network in order to operate the virtual IT systems. If the storage capacities this requires are planned insufficiently, there will be extensive risks regarding the availability of the virtual IT systems and the integrity of the information processed by these systems. This is particularly applicable if special virtualisation functions such as snapshots or the overbooking of storage space are used.

Bottlenecks can involve not only the space available on hard disks or in storage networks, but the internal memory (RAM) or the network connection, as well. Furthermore, insufficient resources on the virtualisation server may result in the virtual machines disrupting one another's operations, which in turn can ultimately cause them to malfunction (or fail entirely).

Information Leaks or Resource Bottlenecks Due to Snapshots

A snapshot may be used to capture and store the condition of a virtual machine. If a snapshot of this kind is restored at a later point in time, all the changes made since it was taken will be lost. As a consequence, any patched vulnerabilities may be reopened. Furthermore, open files,

file transfers or database transactions captured at the time of the snapshot may result in the generation of inconsistent data.

Moreover, attackers might misuse snapshots in order to access the data of a virtual IT system in an unauthorised manner. For example, if a snapshot was made during live operation, the content of the main memory was also saved to the hard disk and may be restored and analysed in a virtual environment outside of the original IT infrastructure. Snapshots can also be large enough to cause a shortage of storage space.

Failure of the Administration Server for Virtualisation Systems

Since the administration server controls and administrates all functions of a virtual infrastructure, a failure of this administration system will make it impossible to perform any configuration changes to the virtual infrastructure. As long as this is the case, the administrators will be unable to react to problems such as resource bottlenecks or the failure of individual virtualisation servers, nor will they be able to integrate new virtualisation servers into the infrastructure or create new virtual IT systems. Live migration (and thus the dynamic assignment of resources for individual guest systems) is also not possible without an administration server.

Misuse of Guest Tools

Guest tools are often executed with very high authorisations. As a consequence, they may be misused for denial-of-service attacks or as a means of taking over the entire host system, for example.

Compromised Virtualisation Software

The virtualisation software (hypervisor) is the central component of a virtualisation server; it controls all virtual machines executed on this server and assigns processor and memory resources to them. If this component is attacked successfully, this will also compromise all the virtual IT systems of the servers.

Requirements

The specific requirements of module SYS.1.5 *Virtualisation* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Head of Networks, Head of IT, Supervisor

Basic Requirements

For module SYS.1.5 *Virtualisation*, the following requirements **MUST** be implemented as a matter of priority:

SYS.1.5.A1 Installation of Updates and Security Updates

The host operating system, management software, and hardware firmware **MUST** be updated at regular intervals. Existing security updates **MUST** be installed in a timely manner. A test system **MUST** be used in advance to check whether the security updates are compatible and do not cause any errors.

SYS.1.5.A2 Secure Use of Virtual IT Systems

Every administrator of virtual IT systems **MUST** know the effects of virtualisation on the IT systems and applications in operation. The access rights of administrators regarding virtual IT systems **MUST** be reduced to those actually required.

It **MUST** be ensured that the network connections which are necessary for the virtual IT systems are available in the virtual infrastructure. It **MUST** also be checked whether the isolation and encapsulation requirements of the virtual IT systems and the applications operated on them are being met. Furthermore, the virtual IT systems used **MUST** meet the requirements regarding availability and data throughput. During live operation, the performance of the virtual IT systems **MUST** be monitored.

SYS.1.5.A3 Secure Configuration of Virtual IT Systems

Guest systems **MAY NOT** access devices and interfaces of the virtualisation server. If a connection of this kind is necessary, it **MUST** be established exclusively and only for the required period of time by the administrator of the host system. Binding rules **MUST** be specified in this regard.

Virtual IT systems **SHOULD** be configured and protected in accordance with the security policies of the organisation (in this regard, see also the modules of the layer *SYS IT Systems* that are appropriate in each case).

SYS.1.5.A4 Secure Configuration of a Network for Virtual Infrastructures

It **MUST** be ensured that existing security mechanisms (e.g. firewalls) and monitoring systems cannot be bypassed by virtual networks. It **MUST** also be ensured that virtual IT systems connected to several networks cannot be used to establish undesired network connections.

Network connections between virtual IT systems and physical IT systems and for virtual security gateways **SHOULD** be configured in accordance with the security policies of the organisation.

SYS.1.5.A5 Protection of Administration Interfaces

All administration and management access to the management system and the host systems **MUST** be restricted. It **MUST** be ensured that it is not possible to access the administration interfaces from non-trustworthy networks.

In order to administer and monitor the virtualisation servers or the management systems, sufficiently encrypted protocols **SHOULD** be used. If non-encrypted (and thus insecure) protocols are nevertheless used, a separate administration network **MUST** be used for the administrators.

SYS.1.5.A6 Logging in the Virtual Infrastructure

The operating condition, usage and network connections of the virtual infrastructure **MUST** be logged continuously. If capacity limits are reached, virtual machines **SHOULD** be relocated and

the hardware SHOULD be extended (if applicable). The log data SHOULD be evaluated regularly.

SYS.1.5.A7 Time Synchronisation in Virtual IT Systems

The system time of all IT systems in production environments MUST be synchronous at all times (see also OPS.1.1.5 *Logging*).

Standard Requirements

For module SYS.1.5 *Virtualisation*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.1.5.A8 Planning a Virtual Infrastructure [Head of IT, Head of Networks]

The structure of the virtual infrastructure SHOULD be planned in detail. In so doing, the applicable rules and policies for operating IT systems, applications, networks and storage networks SHOULD be taken into consideration. If several virtual IT systems are operated on one virtualisation server, there SHOULD be no conflicts regarding the protection needs of the IT systems.

Moreover, the tasks of the individual administrator groups SHOULD be defined and clearly separated. It SHOULD also be defined which employee is responsible for operating which component. The administrators SHOULD be sufficiently qualified.

SYS.1.5.A9 Network Planning for Virtual Infrastructures [Head of IT, Head of Networks]

The structure of the network for virtual infrastructures SHOULD be planned in detail. In this regard, module NET.1.1 *Network Architecture and Design* SHOULD be considered. Whether a separate network must be established and used for certain virtualisation functions (such as live migration) SHOULD also be checked.

It SHOULD be planned which network segments must be established (e.g. management network, storage network) and how these can be separated and protected. In so doing, it SHOULD be ensured that the production network is separated from the management network (see SYS.1.5.A11 *Administration of the Virtualisation Infrastructure Using a Separate Management Network*). The availability requirements for the network SHOULD also be observed and met.

SYS.1.5.A10 Introduction of Management Processes for Virtual IT Systems [Head of IT]

For virtualisation servers and virtual IT systems, processes for commissioning, inventory, operation and decommissioning SHOULD be defined and established. The processes SHOULD be documented and updated at regular intervals.

If such use is planned, it SHOULD be defined which virtualisation functions may be used by the virtual IT systems.

Before a virtual IT system is operated, a test and development environment SHOULD be used to check whether it is suitable for production use. Test and development environments SHOULD not be operated on the same virtualisation server as virtual IT systems in production use.

SYS.1.5.A11 Administration of the Virtualisation Infrastructure Using a Separate Management Network

The virtualisation infrastructure SHOULD only be administered using a separate management network. The available security mechanisms of the management protocols used for authentication, integrity protection and encryption SHOULD be enabled, and all insecure management protocols SHOULD be disabled (see NET.1.2 *Network Management*).

SYS.1.5.A12 Rights and Role Concept for Virtual Infrastructure Administration

Based on the tasks and roles defined in the planning phase (see SYS.1.5.A8 *Planning a Virtual Infrastructure*), a rights and role concept SHOULD be drawn up and implemented for administering virtual IT systems and networks on virtualisation servers and in the management environment. All components of the virtual infrastructure SHOULD be integrated into a central identity and authorisation management system.

Administrators of virtual machines and administrators of the virtualisation environment SHOULD be differentiated and assigned different access rights.

Furthermore, the management environment SHOULD be able to group virtual machines in order to introduce an appropriate structure in connection with corresponding administrator role assignment.

SYS.1.5.A13 Selection of Suitable Hardware for Virtualisation Environments

The hardware used SHOULD be compatible with the virtualisation solution used. Here, it SHOULD be ensured that the manufacturer of the virtualisation solution will also offer support for the hardware operated for the scheduled period of deployment.

SYS.1.5.A14 Uniform Configuration Standards for Virtual IT Systems [Head of IT]

Uniform configuration standards SHOULD be defined for the virtual IT systems used. The virtual IT systems SHOULD be configured in accordance with this standard. The configuration standards SHOULD be reviewed regularly and adapted as required.

SYS.1.5.A15 Operation of Guest Operating Systems with Different Protection Needs

If virtual IT systems with different protection needs are operated jointly on one and the same virtualisation server, it SHOULD be ensured that the virtual IT systems are encapsulated and isolated sufficiently. The network separation of the virtualisation solution used SHOULD be sufficiently secure in this case, as well. If this is not the case, further security safeguards SHOULD be identified and implemented.

SYS.1.5.A16 Encapsulation of Virtual Machines

The functions for copying and pasting information between virtual machines SHOULD be disabled.

SYS.1.5.A17 Monitoring the Operating Condition and Configuration of the Virtual Infrastructure

The operating condition of the virtual infrastructure SHOULD be monitored. In so doing, it SHOULD be checked, for example, whether sufficient resources are still available and whether there might be conflicts in the joint use of resources on a virtualisation server.

Furthermore, it SHOULD be ensured that the configuration files of the virtual IT systems are regularly checked for unauthorised modifications. It SHOULD also be monitored whether the virtual networks have been assigned properly to the respective virtual IT systems.

If configuration changes are performed regarding the virtualisation infrastructure, these SHOULD be checked and tested prior to being implemented.

SYS.1.5.A18 Training of Administrators of Virtual Environments [Supervisor, Head of IT, Head of Networks]

All administrators of the virtual environment SHOULD have received sufficient training. The training courses SHOULD convey how virtual infrastructures can be designed and operated securely.

SYS.1.5.A19 Regular Audits of Virtualisation Infrastructure

There SHOULD be regular audits of whether the actual condition of the virtual infrastructure corresponds to the condition defined in the planning phase and whether the configuration of the virtual components meets the specified default configuration. The audit results SHOULD be documented in a transparent manner. Deviations SHOULD be eliminated.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.1.5 *Virtualisation* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.1.5.A20 Use of Highly Available Architectures [Head of IT, Head of Networks] (A)

The virtual infrastructure SHOULD be designed for high availability. All virtualisation servers SHOULD be consolidated in clusters.

SYS.1.5.A21 Secure Configuration of Virtual IT Systems for Increased Protection Needs (IA)

For virtual IT systems, overbooking features for resources SHOULD be disabled.

SYS.1.5.A22 Hardening of the Virtualisation Server (CI)

The virtualisation server SHOULD be hardened. In order to further isolate and encapsulate virtual IT systems from each other and from the virtualisation server, mandatory access controls SHOULD be used. The IT system on which the management software is installed SHOULD also be hardened.

SYS.1.5.A23 Restriction of Rights of Virtual Machines (CI)

All interfaces and communication channels that make it possible for a virtual IT system to request and obtain information about the host system SHOULD be disabled or suppressed. Furthermore, only the virtualisation server SHOULD be able to access its resources. Moreover, it SHOULD NOT be possible for virtual IT systems to share "pages" of the internal memory.

SYS.1.5.A24 Disabling Snapshots of Virtual IT Systems (CIA)

The snapshot feature SHOULD be disabled for all virtual IT systems.

SYS.1.5.A25 Minimal Use of Console Access to Virtual IT Systems (A)

Direct access to the emulated consoles of virtual IT systems SHOULD be reduced to a minimum. The virtual systems SHOULD be controlled using the network whenever possible.

SYS.1.5.A26 Use of a PKI [Head of IT, Head of Networks] (CIA)

Since communication between the components of the IT infrastructure is mostly secured with the help of certificates, a public-key infrastructure (PKI) SHOULD be used.

SYS.1.5.A27 Use of Certified Virtualisation Software [Head of IT] (CIA)

Certified virtualisation software of the EAL 4 layer or higher SHOULD be used.

SYS.1.5.A28 Encryption of virtual IT systems (CI)

All virtual IT systems SHOULD be encrypted.

Additional Information

For more information about threats and security safeguards for module SYS.1.5 *Virtualisation*, see the following publications, among others:

[CSE113]	Server-Virtualisierung [Server Virtualisation]: BSI publications on Cyber Security (BSI-CS 113, Version 1.0., March 2015, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_113.htm , last accessed on 05.09.2018
[ISFSY13]	The Standard of Good Practice for Information Security: Area SY1.3 - Virtual Servers, Information Security Forum (ISF), June 2018
[NIST800125]	Guide to Security for Full Virtualization Technologies: NIST Special Publication 800-125, January 2011, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-125.pdf , last accessed on 15.08.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.1.5 *Virtualisation*:

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0.1 5	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 5	G 0.2 6	G 0.2 7	G 0.2 8	G 0.2 9	G 0.3 0	G 0.3 1	G 0.3 2	G 0.4 0	G 0.4 3	G 0.4 6
SYS.1.5.A1								X		X	X							
SYS.1.5.A2													X		X			
SYS.1.5.A3						X	X		X	X								
SYS.1.5.A4						X	X											
SYS.1.5.A5	X					X	X						X					
SYS.1.5.A6								X	X	X								
SYS.1.5.A7									X									
SYS.1.5.A8		X								X		X	X	X				
SYS.1.5.A9	X	X				X	X			X			X					
SYS.1.5.A10		X	X	X	X				X									
SYS.1.5.A11	X				X		X											
SYS.1.5.A12		X											X		X			
SYS.1.5.A13		X							X									
SYS.1.5.A14			X		X	X	X											
SYS.1.5.A15						X	X						X				X	
SYS.1.5.A16						X	X						X					
SYS.1.5.A17								X	X	X								

SYS.1.5.A1 8			X											X			
SYS.1.5.A1 9			X			X	X		X								
SYS.1.5.A2 0								X	X							X	
SYS.1.5.A2 1									X	X							
SYS.1.5.A2 2			X		X	X	X										
SYS.1.5.A2 3						X	X										
SYS.1.5.A2 4						X	X						X				
SYS.1.5.A2 5									X	X							
SYS.1.5.A2 6	X				X	X	X									X	
SYS.1.5.A2 7	X			X	X	X	X										
SYS.1.5.A2 8	X																X



SYS.1.7: IBM Z System

Description

Introduction

IBM Z systems belong to the server systems generally referred to as mainframes. Mainframes have developed from classic stand-alone systems with batch processing to state-of-the-art client/server systems. The Z architecture is the successor to the S/360 architecture introduced in 1964 and is often used nowadays in mainframe installations.

Objective

The objective of this module is to protect information which is processed, provided or transmitted via Z systems.

Not in Scope

The module SYS.1.1 *General Server* forms the basis for the protection of server systems. For Z systems, both the general requirements listed there and the concrete requirements in this module must be considered.

Different operating systems are available for the Z hardware (e.g. z/OS, VSE, z/VM or Linux). These are normally selected based on the computer size and purpose at hand. The recommendations of this module are essentially limited to the operating system z/OS. Select security aspects of z/VM are also addressed. For the Linux operating system, please refer to the module SYS.1.3 *Unix Servers*.

An important component of the security concept of Z systems at the technical level is the security system used – for example, TopSecret, ACF2 or RACF. To simplify the information presented, only RACF is discussed below. The recommendations should be adapted accordingly if a different security system is used.

The respective specific services offered by the Z system are not part of this module. For these services, additional modules will need to be created based on the results of the IT-Grundschutz modelling process.

Threat Landscape

For module SYS.1.7 *IBM Z System*, the following specific threats and vulnerabilities are of particular importance:

Inadequate or Incorrect Configuration of the Hardware or the z/OS Operating System

The configuration of a z/OS operating system is very complex and requires considerable intervention by a system administrator. Incorrect or inadequate configuration can rapidly produce vulnerabilities that can lead to related security problems. Supervisor calls (SVCs) are, for example, calls to special z/OS utilities that run with a high level of authorisation in kernel mode. Under certain circumstances, insecure SVC programs can be used to circumvent z/OS security mechanisms.

Incorrect Configuration of the z/OS Security System, RACF

In a z/OS operating system, a special security system is responsible for authenticating users and authorising them to access resources. Resource Access Control Facility (RACF) is often used for this purpose. As a rule, the default configuration of RACF does not match the security requirements in the related operational scenario. The resources and z/OS system commands are protected using special classes in RACF, for example. If these classes are inadequately defined, it is possible for users to issue system commands that could degrade stable system operation in certain circumstances.

Incorrect Use of the z/OS System Functions

Due to the complexity of a z/OS operating system and its components, operating errors cannot be ruled out completely. Depending on the nature of an incorrect action, individual components or the entire system may fail. For example, if different resources lock one another (contention), functions may not be available until the lock is removed. Often a series of system prompts (displays) and considerable experience are necessary to remove the mutual locks with the aid of the right MVS commands.

Manipulation of the z/OS System Configuration

z/OS systems can be influenced via various interfaces, such as the hardware management console, local/remote MCS consoles, automation procedures and remote maintenance access. For example, if physical or logical access to remote MCS consoles is inadequately protected, z/OS systems may be tampered with from there.

Attacks on z/OS Systems Using TCP/IP

To attack a z/OS system over the network connection, it is often not necessary to have any special knowledge of the network architecture or z/OS. Due to the TCP/IP connection to (in some circumstances public) networks and the Unix system services, many z/OS systems can be reached by external attackers using standard protocols and services such as HTTP or FTP. External attackers can, in certain circumstances, carry out denial-of-service attacks against the services provided over the TCP/IP connection to public networks or read or tamper with transmitted data without authorisation. Internal attackers can try to increase their authorisations using the TCP/IP connection to internal networks by obtaining, for instance, the ID and password for a user with SPECIAL rights.

Incorrect Character Conversion When Using z/OS

EBCDIC, ASCII, and Unicode are character sets that determine how letters, numbers and other characters are represented by bits. z/OS systems work with EBCDIC code. Only HFS and zFS file systems used with Unix System Services (USS) make it possible to save data in both ASCII and EBCDIC. When exchanging data between z/OS systems and systems using ASCII or Uni-

code (including from USS to MVS, for example), there is a risk that information could be corrupted if incorrect translation tables (code page translation) are used. Here, the translation of special characters is a particularly frequent problem.

Requirements

The specific requirements of module *SYS.1.7 IBM Z System* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Human Resources Department, IS Audit Team, Head of IT

Basic Requirements

For module *SYS.1.7 IBM Z System*, the following requirements **MUST** be implemented as a matter of priority:

SYS.1.7.A1 Use of restrictive z/OS IDs

High-level authorisations **MAY** only be assigned to users who need these rights for their activities. In particular, the RACF attributes SPECIAL, OPERATIONS, AUDITOR and the corresponding GROUP attributes, as well as the user ID 0, **MUST** be handled restrictively under Unix System Services (USS). The assignment and use of these authorisations **MUST** be documented transparently. The special identifier IBMUSER **MAY** be used during reinstallation to create identifiers with SPECIAL attributes. Once this is complete, it **MUST** be permanently disabled. To prevent administrators from permanently locking themselves out, an emergency user procedure **MUST** be set up.

SYS.1.7.A2 Protection of security-critical z/OS utilities

Security-critical programs and commands and their alias names **MUST** be protected with rights to corresponding RACF profiles in such a way that they can only be used by the designated and authorised employees. It **MUST** be ensured that (third-party) programs cannot be installed without authorisation. In addition, programs **MAY** only be installed from secured sources using transparent methods (e.g. SMP/E).

SYS.1.7.A3 Maintenance of Z systems

The Z hardware and firmware, the operating system and the various program products **MUST** be maintained regularly and as required. The maintenance activities required for this **MUST** be planned and integrated into change management (see OPS.1.1.3 *Patch and Change Management*). In particular, updates **MAY** only be performed by the manufacturer under the control of the operator, locally via SE (Support Elements) or HMC (Hardware Management Console), or remotely via the RSF (Remote Support Facility) remote control console.

SYS.1.7.A4 Training z/OS operators [Human Resources Department]

Administrators, operators and auditors with tasks related to z/OS MUST be trained according to these tasks. In particular, RACF administrators MUST be familiar with the security system itself and any other functions relevant to it.

SYS.1.7.A5 Use and protection of system-related z/OS terminals

System-adjacent z/OS terminals MUST be physically and logically protected against unauthorised access. The Support Elements in particular MUST be considered, along with the HMC, MCS, SMCS, Extended MCS and monitor consoles. Preset passwords MUST be changed. Web servers and other forms of remote access MUST be disabled when not in use.

SYS.1.7.A6 Use and protection of the remote support facility [Head of IT]

Management MUST decide if and how RSF is to be used. Such use MUST be provided for in a maintenance contract and coordinated with hardware support staff. It MUST be ensured that the RSF configuration can only be changed by authorised persons. Maintenance access for firmware modifications by the manufacturer MUST be explicitly approved by the operator and deactivated again after completion. RSF communication MUST take place via secure connections (TLS).

SYS.1.7.A7 Restrictive authorisation in z/OS

In the basic configuration, the authorisation mechanisms MUST be configured so that all persons (defined user IDs in groups according to the respective roles) only have the access options they need for their respective activities. For this purpose, APF (authorised program facility) authorisations, supervisor calls (SVCs), resources of the z/OS operating system, IPL parameters, Parmlib definitions, started tasks and JES2/3 definitions MUST be considered.

SYS.1.7.A8 Use of the z/OS security system RACF

The use of RACF for z/OS MUST be planned. This includes the selection of a character set, the definition of rules for user IDs and passwords and the activation of KDFAES encryption. Preset passwords (e.g. for the RVARY command, but also for newly created user IDs) MUST be changed. If RACF exits are to be used, they MUST be justified, documented and regularly monitored.

Suitable procedures MUST be defined for creating, locking, releasing and deleting RACF IDs. After a specified number of failed login attempts, a RACF ID MUST be locked (exception: emergency user procedure). User identifiers MUST also be blocked after a prolonged period of inactivity, but process identifiers must not.

Files, started tasks and security-critical programs MUST be protected with RACF profiles. Users MAY only get the data access they need in accordance with their role. It MUST also be ensured that they are not able to extend their access options without permission.

SYS.1.7.A9 Multi-client capability in z/OS

If a z/OS system is to be used by clients, a RACF concept for client separation MUST be created. The data and applications of the clients MUST be segregated through RACF profiles. High-level authorisations in RACF (SPECIAL, OPERATIONS, AUDITOR) and change access to files of the z/OS operating system MAY only be granted to employees of the operator. The maintenance time slots in which the z/OS system will not be available MUST be co-ordinated with all the clients working on the system concerned.

SYS.1.7.A10 Protecting the login process in z/OS

It **MUST** be ensured that only authorised persons can log on to z/OS systems or otherwise gain access. The authorised persons **MUST** be defined in advance. Services and ports that are not required **MUST** be disabled or blocked. In cases where z/OS systems are to be accessed from public networks, the possibility that all the IDs can be blocked through the incorrect entry of passwords **MUST** be prevented (emergency user procedure).

SYS.1.7.A11 Protection of session data

Session data for the connections of the RACF administrators and other employees **MUST** be transferred in encrypted form.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module *SYS.1.7 IBM Z System*: They **SHOULD** be implemented as a matter of principle.

SYS.1.7.A12 Planning Z systems [Head of IT]

The use of Z systems **SHOULD** be planned comprehensively. The manner in which Z systems are to be installed at a data centre, how hardware is to be scaled, which operating systems are to be used and which requirements will be placed on the applications **SHOULD** be determined. Integration into the organisation's processes, compliance with security regulations and the deployment of qualified personnel **SHOULD** also be considered during the planning.

SYS.1.7.A13 Drawing up a security policy for z/OS systems

Before using z/OS systems, appropriate security policies **SHOULD** be planned and established. Integration into security management, user administration, authorisation management and a reporting and escalation procedure **SHOULD** be regulated. Technical aspects such as emergency systems and emergency users, RACF databases, checking/monitoring and check lists for security settings **SHOULD** be taken into account.

SYS.1.7.A14 Reporting for secure operation of z/OS

A process **SHOULD** therefore be set up to monitor all security-relevant operations. This **SHOULD** specify the security reports to be produced regularly, the tools and data sources to be used (e.g. system management facility) and how deviations from the specifications are to be dealt with. The security reports **SHOULD** be used as information during checks.

SYS.1.7.A15 Checking the secure operation of z/OS [IS Audit Team]

Regular checks **SHOULD** be carried out to ensure compliance with the required security settings and procedures (pre-audit). The auditors **SHOULD** be independent and have the necessary knowledge and data access rights. The checks **SHOULD** at least cover the security-critical settings, events and actions. In addition, indications of potential security breaches **SHOULD** be investigated.

SYS.1.7.A16 Monitoring of z/OS systems

During operation, the z/OS system **SHOULD** be monitored for important messages, events and compliance with limit values. In particular, error messages on the HMC console, WTOR and important WTO messages (write to operator/with reply), system tasks, security breaches, capacity limits, and system utilisation **SHOULD** be considered. For monitoring, at least the MCS console, the system management facility, the SYSLOG and the relevant log data of the applica-

tions SHOULD also be used. It SHOULD be ensured that all important messages are recognised promptly and responded to in an appropriate manner when required. System messages SHOULD be filtered in such a way that only those messages that are actually important are displayed.

SYS.1.7.A17 Synchronisation of z/OS passwords and RACF commands

If z/OS passwords or RACF commands are to be automatically synchronised across several z/OS systems, the respective systems SHOULD be standardised as far as possible. The blocking of user IDs due to incorrect password entries SHOULD NOT be synchronised. The risk of synchronising security-critical RACF commands SHOULD be taken into account. The management function of the synchronisation programme SHOULD only be available to authorised employees within the scope of their activities.

SYS.1.7.A18 Role concept for z/OS systems

A role concept SHOULD be introduced for the system administration of z/OS systems at minimum. Arrangements for deputies SHOULD also be in force for all important system administration roles. The RACF attributes SPECIAL, OPERATIONS and AUDITOR SHOULD be assigned to different people (role separation).

SYS.1.7.A19 Protection of z/OS transaction monitors

If transaction monitors or databases such as IMS, CICS or DB2 are used in z/OS, they SHOULD be backed up using RACF. This also applies to the associated MVS commands and files. Internal security mechanisms for transaction monitors and databases, on the other hand, SHOULD only be used where there are no corresponding RACF functions. Users and administrators SHOULD only receive the access rights they need for their respective tasks.

SYS.1.7.A20 Decommissioning of z/OS systems

When decommissioning z/OS systems, hard disks containing sensitive data SHOULD be erased in such a way that their contents cannot be reproduced. Other z/OS systems, groupings and management systems SHOULD be adapted so that they no longer refer to the decommissioned system. The impact on software licenses SHOULD also be considered.

In the event that defective hard disks are replaced by the manufacturer, it SHOULD be contractually agreed that these hard disks will be securely destroyed or deleted in such a way that their contents can no longer be reproduced.

SYS.1.7.A21 Protection of the startup process of z/OS systems

The parameters necessary for the startup procedure of a z/OS system SHOULD be documented and known to the operating personnel. The required hardware configurations, such as the IOCDS file (Input/Output Configuration Data Set) and the LPARs (logical partitions), SHOULD also be available. An MVS master console and a backup console SHOULD be defined to control messages. After the startup procedure, a check list SHOULD be used to check whether the system status corresponds to the target specifications. In addition, a fallback configuration with which the system was successfully started before the last change SHOULD be maintained.

SYS.1.7.A22 Protection of the operating functions of z/OS

All maintenance work affecting production, as well as dynamic and other changes, SHOULD only be carried out within the framework of change management (see OPS.1.1.3 *Patch and Change Management*). SDSF (System Display and Search Facility) and similar functions, as well as priority control for jobs, SHOULD be protected against unauthorised access. z/OS system

commands and particularly security-relevant commands for dynamic changes SHOULD be protected via RACF. When defining hardware dynamically, it SHOULD be ensured that a resource is not assigned to several individual systems outside a Parallel Sysplex during actual operation.

SYS.1.7.A23 Protection of z/VM

If z/VM is used, this product SHOULD be integrated into patch management. All preset passwords SHOULD be changed. The role of z/VM system administrator SHOULD only be assigned to persons who require these authorisations. RACF for z/VM SHOULD be used for z/VM security administration. z/VM system commands that are critical to security SHOULD be protected using RACF. The virtual machines defined in z/VM SHOULD only be provided with the resources necessary to perform their particular tasks and strictly separated from each other. Only the services needed SHOULD be started in z/VM. When checks are performed, the journaling function of z/VM and the audit functions of RACF SHOULD be used.

SYS.1.7.A24 Administration of storage media in z/OS systems

Files, programs and functions for the administration of storage media – as well as the storage media themselves (hard disks and tapes), including the master catalogue – SHOULD be protected using RACF profiles. Backup copies of all important files SHOULD be available that can be installed in case of an emergency. The assignment of storage media to Z systems SHOULD be documented transparently. It SHOULD be ensured that sufficient tape stations are available for the volume and time frame at hand. The disks that are to be backed up and how the backup is to be carried out SHOULD be specified when using the HSM (Hierarchical Storage Manager). Tapes that are managed by the HSM SHOULD NOT be edited elsewhere.

SYS.1.7.A25 Stipulation of z/OS system capacity

The limits for maximum resource load (number of CPUs, storage, bandwidth, etc) SHOULD be set according to the hardware requirements and made known to the administrators and application owners affected. The number of magnetic tape stations available, the times during which applications access the magnetic tape stations and the required disk capacities SHOULD be agreed with the application owners. The hard disk capacities SHOULD also be monitored by space management.

SYS.1.7.A26 Workload management for z/OS systems

The programs, files and commands of the Workload Manager (WLM), as well as the necessary couple data sets, SHOULD be protected by RACF. It SHOULD be ensured that the authorisations required to change the WLM via MVS commands and via the SDSF interface are the same.

SYS.1.7.A27 Character set conversion in z/OS systems

When text files are transferred between z/OS systems and other systems, it SHOULD be taken into account that character set conversion may be required. The correct conversion table SHOULD be used for this. When transferring program source code, the correct translation of characters SHOULD be checked. When transmitting binary data, on the other hand, it SHOULD be ensured that no character set conversion takes place.

SYS.1.7.A28 Licence key management for z/OS software

For licence keys with limited validity, a timely renewal procedure SHOULD be put in place. The contract periods of the licence keys SHOULD be documented. The documentation SHOULD be made available to all the administrators concerned.

SYS.1.7.A29 Protection of unix system services on z/OS systems

The parameters of Unix System Services (USS) SHOULD be set according to the functional and security specifications at hand while also taking the available resources into account. HFS and zFS files containing USS file systems SHOULD be backed up via RACF profiles and included in the backup concept. The root file system SHOULD also be mounted with the read-only option. In the USS file system, APF (authorised program facility) authorisations SHOULD never be granted using a file security packet (FSP). The modules of APF files of the z/OS operating system SHOULD be loaded instead. The assignment between USS user IDs and MVS user IDs SHOULD be clear. Authorisations under USS SHOULD be assigned using the RACF class UNIX-PRIV and not by assigning UID 0. The USS SHOULD be checked and monitored using the same mechanisms used for z/OS.

SYS.1.7.A30 Protection of the z/OS trace functions

The trace functions of z/OS, such as GTF (generalised trace facility), NetView or ACF/TAP (Advanced Communication Function/Trace Analysis Program) and the corresponding files, SHOULD be protected in such a way that only the responsible and authorised employees have access to them. The trace function of NetView SHOULD be disabled in normal circumstances and only activated if required.

SYS.1.7.A31 Contingency planning for z/OS systems

In the event that all identifiers with SPECIAL rights are blocked or no RACF administrator is available in an emergency situation, an emergency user procedure SHOULD be set up. A procedure SHOULD also be established for recovering a functioning RACF database. Furthermore, a copy of the z/OS operating system SHOULD be kept as a z/OS backup system and a z/OS business continuity system maintained in a manner independent from the production system.

Requirement in Case of Increased Protection Needs

Generic suggestions for module *SYS.1.7 IBM Z System* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.1.7.A32 Determining standards for z/OS system definitions (CIA)

Standards and naming conventions for z/OS system definitions SHOULD be defined and documented. The documentation SHOULD be made available to all the administrators. Regular checks SHOULD be performed to ensure that the standards are followed. Standards SHOULD be defined for file, database, job and volume names in particular, as well as for application, system and user IDs.

SYS.1.7.A33 Separation of test and production systems in z/OS (CIA)

Technical measures SHOULD be taken to separate development and test systems from production systems in z/OS. Possible access options to shared hard disks and the Parallel Sysplex SHOULD be taken into account.

SYS.1.7.A34 Batch job planning for z/OS systems (A)

If a z/OS system processes a large number of batch jobs, a job scheduler SHOULD be used for batch job flow control. The job scheduler and the associated files and tools SHOULD be suitably protected by RACF.

SYS.1.7.A35 Use of RACF exits (CI)

If RACF exits are to be used, the security and operational consequences SHOULD be analysed. The RACF exits SHOULD also be installed and monitored via the SMP/E (System Modification Program/Enhanced) as USERMOD.

SYS.1.7.A36 Internal Communication between operating systems (CIA)

The communication between operating systems – e.g. z/OS and Linux, which are either installed in LPAR mode or under z/VM on the same Z hardware – SHOULD be performed over internal channels, i.e. HiperSockets or virtual channel-to-channel (CTC) connections.

SYS.1.7.A37 Parallel Sysplex in z/OS (A)

Based on availability and scalability requirements, a decision SHOULD be made as to whether a Parallel Sysplex (a cluster of z/OS systems) is to be used and, if so, which redundancies are to be provided. The requirements of the applications SHOULD be taken into account when planning the capacity of the necessary resources. The software and the definitions of the LPARs of the Sysplex, including RACF, SHOULD be synchronised or provided as shared files.

It SHOULD be ensured that all LPARs of the Sysplex can access the couple data sets. The couple data sets, as well as all security-critical programs and commands for managing the Sysplex, SHOULD be protected by RACF. A GRS (global resource serialisation) network SHOULD also be set up. The hard disks of the Sysplex SHOULD be strictly separated from the hard disks of other systems. The system logger SHOULD be used with staging data sets.

SYS.1.7.A38 Use of the VTAM session management exit in z/OS (CI)

If a VTAM session management exit is to be used, it SHOULD be ensured that it will not impair secure and efficient operation. The exit SHOULD allow at least a subsequent check of a rejected login attempt. In addition, the exit SHOULD be configured dynamically and the set of rules loaded from an external file. Functions, commands and files related to the exit SHOULD be protected by RACF.

Additional Information

Interesting Facts

A number of abbreviations that are not explained elsewhere in IT-Grundschutz are commonly used in the Z system environment. These include:

MVS: MVS (Multiple Virtual Storage) was a predecessor of the current z/OS operating system

HMC (Hardware Management Console), MCS (Multiple Console Support), SMCS, Extended MCS: consoles for monitoring and controlling a Z system or z/OS operating system

HFS: Hierarchical File System

IPL: Initial Program Load, the startup procedure of an operating system

RSF: Remote Support Facility, a remote control console

SE: Support Elements, for system configuration and control

SMP/E: System Modification Program/Extended, a software installation procedure

zFS: zSeries File System, a file system used in z/OS and Unix System Services (USS)

References

For more information about threats and security safeguards for module “SYS.1.7 *IBM Z System*”, see the following publications, among others:

[IBM]	ABC of z/OS System Programming Volume 1-13: IBM Redbooks, https://www.redbooks.ibm.com , last accessed on 05.10.2018
-------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.1.7 *IBM Z System*:

- G 0.14 Interception of Information / Espionage
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.33 Shortage of Personnel
- G 0.36 Identity Theft
- G 0.37 Repudiation of Actions
- G 0.39 Malware

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	Re-quirements	G 0.1 4	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 5	G 0.2 6	G 0.2 7	G 0.2 8	G 0.3 0	G 0.3 1	G 0.3 2	G 0.3 3	G 0.3 6	G 0.3 7	G 0.3 9	G 0.4 0	G 0.4 3	G 0.4 5	G 0.4 6
SYS.1 .7.A1		X		X		X	X	X					X		X		X	X		X		X	X
SYS.1 .7.A2		X		X		X	X	X					X		X		X	X		X		X	X
SYS.1 .7.A3					X	X	X	X	X	X		X	X							X	X	X	X
SYS.1 .7.A4			X	X										X								X	X
SYS.1 .7.A5		X		X		X	X	X					X								X	X	X
SYS.1 .7.A6		X		X	X	X	X	X					X				X				X	X	X
SYS.1 .7.A7		X		X		X	X	X					X		X		X	X				X	X
SYS.1 .7.A8		X	X	X		X	X	X					X		X		X	X	X			X	X
SYS.1 .7.A9		X	X	X		X	X						X	X	X		X	X	X		X	X	X
SYS.1 .7.A1 0		X		X			X	X					X							X	X	X	X
SYS.1 .7.A1 1		X		X				X					X		X		X	X			X		
SYS.1 .7.A1 2			X							X				X		X							

SYS.1 .7.A1 3		X	X									X	X	X						X	X	
SYS.1 .7.A1 4	X	X	X		X	X						X	X	X		X	X	X	X	X	X	X
SYS.1 .7.A1 5	X	X	X		X	X						X	X	X		X	X	X	X	X	X	X
SYS.1 .7.A1 6	X	X	X		X	X	X	X	X	X		X	X	X		X	X	X	X	X	X	X
SYS.1 .7.A1 7		X						X	X				X								X	
SYS.1 .7.A1 8		X							X				X		X							
SYS.1 .7.A1 9	X		X		X	X	X					X		X		X	X				X	X
SYS.1 .7.A2 0		X	X				X		X						X							
SYS.1 .7.A2 1		X						X	X				X		X							
SYS.1 .7.A2 2	X	X	X		X	X	X	X	X			X	X	X		X	X				X	X
SYS.1 .7.A2 3	X	X	X	X	X	X	X				X	X	X	X		X	X		X		X	X
SYS.1 .7.A2 4	X	X	X		X	X	X		X	X		X		X		X	X	X			X	X
SYS.1 .7.A2 5		X						X	X	X			X								X	

SYS.1 .7.A2 6			X		X	X	X	X	X	X		X		X	X				X	X		
SYS.1 .7.A2 7		X						X	X		X								X	X		
SYS.1 .7.A2 8		X						X	X	X												
SYS.1 .7.A2 9	X		X		X	X	X	X	X	X		X		X	X				X	X		
SYS.1 .7.A3 0	X		X				X					X		X				X				
SYS.1 .7.A3 1		X						X	X			X		X				X		X		
SYS.1 .7.A3 2		X										X										
SYS.1 .7.A3 3	X		X	X	X	X	X	X	X		X	X	X	X		X	X	X		X	X	X
SYS.1 .7.A3 4	X	X	X		X	X	X	X	X	X		X		X	X				X	X		
SYS.1 .7.A3 5	X		X		X	X	X	X	X		X		X		X	X			X	X		
SYS.1 .7.A3 6	X		X			X	X			X					X	X	X	X	X		X	
SYS.1 .7.A3 7		X						X	X	X								X		X		
SYS.1 .7.A3 8	X		X			X	X					X						X	X	X	X	



SYS.1.8: Storage Solutions

Description

Introduction

The constant growth of digital information and the increasing amount of non-structured information are prompting organisations to implement central storage solutions. The requirements for such storage solutions are subject to constant change; this can be seen, for example, in the following aspects:

- The data of an organisation should be available at any time and place for various application scenarios. This is why state-of-the-art storage solutions are often subject to more stringent availability requirements.
- The increasing digitalisation of all information within an organisation also makes it necessary to consider and comply with a multitude of legal requirements (compliance).
- Storage solutions should be dynamically adaptable to the continuously changing requirements and able to provide storage space in a centralised manner.

In the past, storage solutions were often implemented by connecting storage media directly to a server. However, these direct-attached storage (DAS) systems are often no longer able to meet the current and future requirements. This has led to the necessity for the central storage solutions commonly used today (and their components). They are differentiated as follows:

- Storage solution: this consists of one or several storage networks and at least one storage system.
- Storage network: this enables access to the storage systems and the replication of data between storage systems.
- Storage system: a central instance that provides the other IT systems with storage space. A storage system also allows multiple IT systems to access the available storage space simultaneously.

Objective

The objective of this module is to show how central storage solutions can be planned, operated and decommissioned in a secure manner.

Not in Scope

This module addresses storage systems together with the related storage networks. Backup devices connected to the storage system or to the storage network are not addressed here; they are addressed in module OPS.1.2.2 *Archiving*. Conceptual aspects of backups are explained in module CON.3 *Backup Concept*. Furthermore, no requirements regarding file servers are described. These can be found in module APP.3.3 *File Servers*.

If external service providers are used in order to operate a storage solution, the requirements of module OPS.2.1 *Outsourcing for Customers* must be taken into consideration separately.

Threat Landscape

For module SYS.1.8 *Storage Solutions*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Delimitation of Responsibilities Regarding Storage Solutions

Central storage solutions lead to increased requirements in the field of administration. If the responsibilities for different areas are not defined unambiguously in this regard, incorrect configurations may be the result. For example, if a classic network administrator administers fibre channel (FC) switches, they may access components for which they are neither responsible nor trained. This may result in FC switches being configured improperly. As a consequence, important services might fail because all servers connected to the FC switches are no longer able to access the storage systems.

Insecure Default Settings for Storage Components

Storage components are frequently delivered with a default configuration that makes it possible to commission the devices quickly and with as many functions as possible. Unnecessary features (such as HTTP, Telnet, and insecure SNMP versions) are thus enabled in many devices. If storage components with insecure factory settings are used in production environments, it is easier to access them without authorisation. This may result in services, for example, being no longer available or confidential information of the organisation being accessed without authorisation.

Manipulation of Data via the Storage System

Networks can use a poorly configured storage area network (SAN) to establish unwanted connections. For example, if a server with an SAN connection is available from the Internet and can be compromised from the outside, the server may be used as an entrance point for attackers in order to access sensitive information stored in the SAN without authorisation. Since all security and monitoring safeguards in the IT networks of an organisation (such as firewalls or intrusion detection systems, IDS) may be bypassed this way, the potential scale of damage is high.

Loss of Confidentiality Due to Storage-Based Replication Methods

The purpose of storage-based replication methods is to duplicate stored or archived data in real time via a storage network in order to achieve additional redundancy. This helps to avoid data losses. Automated replication of unencrypted data, however, involves risks both in the company's own network and when using public networks: for example, legitimate replication

traffic can be accessed without authorisation using FC analysers (FC replication) or sniffers (IP replication).

Access to Information of Other Clients Using WWN Spoofing

Devices in an FC-SAN are managed and assigned internally using world wide names (WWNs). They are similar in some ways to the MAC addresses of Ethernet network adapters. Using programs made available by the manufacturer of the host bus adapters (HBA), the WWN of an HBA may be changed. The attacker may thus access data without corresponding authorisation. The manipulation of WWNs, also referred to as WWN spoofing, poses a considerable damage risk to an organisation. Particularly in connection with multi-client-capable storage systems, unauthorised persons may access the information of other clients.

Bypassing Logical Network Separation

If the network structures of different clients are separated not by physically separate networks, but by virtual storage area networks (VSANs), the information security of the organisation may be endangered as a consequence. If an attacker manages to penetrate the network of another client, they may access the virtual SAN of this client and the payload transferred.

Failure of Storage Solution Components

Complex, network-based storage solutions often consist of many components (e.g. FC switches, storage controllers, virtualisation appliances). If components of a storage solution fail, this may result in important applications no longer working properly and data being lost.

Obtaining Physical Access to SAN Switches

If the site and system access controls for the components of a storage system are insufficient or simply not in place in an organisation, it is possible for an attacker to gain physical access to existing switches or to connect additional FC-SAN switches to the network. The attacker may be seeking to access the distributed zoning database in order to change it and gain access to the storage systems.

Requirements

The specific requirements of module SYS.1.8 *Storage Solutions* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO), Head of IT, Building Services, Supervisor

Basic Requirements

For module SYS.1.8 *Storage Solutions*, the following requirements MUST be implemented as a matter of priority:

SYS.1.8.A1 Appropriate Installation of Storage Systems [Building Services, Head of IT]

The IT components MUST be installed in secured rooms. ONLY authorised persons MAY access these rooms. Furthermore, a secure power supply and an ambient temperature and humidity in line with the manufacturer's specifications MUST be ensured.

SYS.1.8.A2 Secure Basic Configuration of Storage Solutions

Prior to production use of a storage solution, it MUST be ensured that all software and firm-ware components are up to date. Afterwards, a secure basic configuration MUST be established.

User accounts that are not required MUST be deactivated. Default passwords MUST be changed or new accounts created in accordance with the password policy.

Unused interfaces of the storage system MUST be disabled. The default configuration, the basic configuration performed, and the current configuration SHOULD be stored in a secure and redundant manner.

SYS.1.8.A3 Restrictive Granting of Access Rights

A rights and role concept MUST be drawn up for storage solutions. All user accounts created on the respective solution MUST be in accordance with this concept. All user accounts MUST be established in accordance with the principle of the minimal authorisations.

SYS.1.8.A4 Protection of Administration Interfaces

All administration and management access to the storage systems MUST be restricted. It MUST be ensured that it is not possible to access the administration interfaces from non-trustworthy networks.

Sufficiently encrypted protocols SHOULD be used. If non-encrypted (and thus insecure) protocols are nevertheless used, a separate administration network MUST be used for the administrators.

SYS.1.8.A5 Logging in Storage Systems

Internal logging of the storage systems MUST be configured to include information that helps detect problems at an early stage.

Standard Requirements

For module SYS.1.8 *Storage Solutions*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.1.8.A6 Drawing Up a Security Policy for Storage Solutions [Chief Information Security Officer (CISO)] (I)

Based on the general security policy of the organisation, a specific policy SHOULD be drawn up for storage solutions. This policy SHOULD transparently describe requirements and specifica-

tions as to how storage solutions may be planned, administered, installed, configured and operated securely.

The policy SHOULD be known to all administrators in charge of storage solutions and SHOULD be the basis of their work. If the policy is changed or deviations from the requirements are allowed, this SHOULD be coordinated with the CISO and documented. It SHOULD be checked regularly whether the policy is still properly implemented. The results SHOULD be appropriately documented.

SYS.1.8.A7 Planning of Storage Solutions [Chief Information Security Officer (CISO), Head of IT]

A requirements analysis SHOULD be performed that addresses, amongst other things, the subjects of performance and capacity. Based on the requirements identified, a detailed plan for storage solutions should then be drawn up. The following items SHOULD be taken into account:

- selection of suitable hardware
- selection of manufacturers and suppliers
- a decision in favour of or against central management systems
- planning of the network connection
- planning of the infrastructure
- integration into existing processes

SYS.1.8.A8 Selection of an Appropriate Storage Solution [Chief Information Security Officer (CISO), Head of IT] (I)

The technical bases of different storage solutions SHOULD be addressed in a detailed manner and their effects on the possible use in an organisation SHOULD be checked. In so doing, options and limits of the different storage system types SHOULD be illustrated in a transparent manner for the persons in charge in the organisation. The decision criteria for a storage solution SHOULD be documented in a transparent manner. The decision regarding the selection of a storage solution SHOULD also be documented in a transparent manner.

SYS.1.8.A9 Selection of Suppliers for a Storage Solution [Chief Information Security Officer (CISO), Head of IT] (I)

Based on the specified requirements regarding a storage solution, an appropriate supplier SHOULD be selected. The selection criteria and the decision in favour of a supplier SHOULD be documented in a transparent manner. Furthermore, maintenance and repair aspects SHOULD be documented in writing in service level agreements (SLAs). The SLAs SHOULD be unambiguous and quantifiable. The exact scheduled end of the contract with the supplier SHOULD be established in writing.

SYS.1.8.A10 Drawing Up and Maintaining an Operating Manual [Chief Information Security Officer (CISO), Head of IT] (I)

An operating manual SHOULD be drawn up. It SHOULD document all the rules, requirements and settings that are necessary in operating storage solutions. The operating manual SHOULD be updated at regular intervals.

SYS.1.8.A11 Secure Operation of a Storage Solution

The storage system SHOULD be monitored regarding the availability of the internal applications, system utilisation and critical events (see also SYS.1.8.A13 *Monitoring and Management of Storage Solutions*). Furthermore, fixed maintenance windows in which changes may be implemented SHOULD be defined for storage solutions. In particular, firmware or operating system updates to storage systems or the network components of a storage solution SHOULD only be performed within a maintenance window. Any changes SHOULD also be enabled via change management and coordinated with all Process Owners involved.

SYS.1.8.A12 Administrator Training [Supervisor, Head of IT]

The administrators responsible for the storage solutions SHOULD be sufficiently trained. The training sessions SHOULD convey knowledge of the methods, techniques, and tools to be used in order to configure and securely operate storage systems and the related components. Furthermore, manufacturer-specific aspects of individual products and components SHOULD be addressed. If an organisation starts using new products, the administrators SHOULD receive corresponding training.

SYS.1.8.A13 Monitoring and Administration of Storage Solutions

In order to be able to detect and eliminate error situations and security issues, storage solutions SHOULD be monitored. In so doing, all data collected SHOULD be checked as to whether the specifications of the operating manual are being followed (see also SYS.1.8.A10 *Drawing Up and Maintaining an Operating Manual*).

Individual components of the storage solution and the overall system SHOULD be managed in a centralised manner. Moreover, the essential messages SHOULD be filtered out for the sake of better visibility.

If a storage solution is operated by an external service provider, it SHOULD be defined and documented how the contractually stipulated SLAs are to be monitored.

SYS.1.8.A14 Protection of an SAN Through Segmentation

An SAN SHOULD be segmented. A concept SHOULD be drawn up that assigns the SAN resources to the respective servers. In this regard, a decision as to which segmentation is to be used in which deployment scenario SHOULD be made based on the security requirements and the time required for administration. The current resource assignment SHOULD be easily and clearly identifiable with the help of the administration tools. Furthermore, the current zoning configuration SHOULD be documented. The documentation SHOULD also be available in case of emergency.

SYS.1.8.A15 Secure Separation of Clients in Storage Solutions

The organisation's requirements regarding the multi-client capability of a storage solution SHOULD be defined and documented in a transparent manner. The storage solutions used SHOULD meet these documented requirements.

In the block storage environment, LUN masking SHOULD be used in order to separate clients. In file service environments, it SHOULD be possible to use virtual file servers. Here, every client SHOULD be assigned its own file service.

When using IP or iSCSI, the clients SHOULD be separated via segmentation within the network. If fibre channel is being used, VSANs and soft zoning SHOULD be used for segmentation purposes.

SYS.1.8.A16 Secure Deletion in SAN Environments (I)

For the storage system, it SHOULD be defined which information is to be deleted using which procedure. In multi-client-capable storage systems, it SHOULD be ensured that the logical unit numbers (LUNs) assigned to a certain client are deleted.

SYS.1.8.A17 Documenting the System Settings of Storage Systems

All system settings of storage systems SHOULD be documented. The documentation SHOULD include the technical and organisational specifications, as well as any specific configurations of the storage systems of the organisation.

If the documentation of the system settings includes confidential information, this information SHOULD be protected against unauthorised access. The documentation SHOULD be checked regularly and kept up to date at all times, particularly regarding the granting of rights. It SHOULD also be ensured that it is available in all emergency scenarios.

SYS.1.8.A18 Security Audits and Reporting Regarding Storage Systems [Chief Information Security Officer (CISO)] (I)

All storage systems used SHOULD be audited at regular intervals. A corresponding process SHOULD be established. It SHOULD be specified which security reports are to be drawn up at regular intervals and what they are to contain. Furthermore, it SHOULD also be specified how deviations from specifications must be handled and how often and to what extent audits are to be performed.

SYS.1.8.A19 Decommissioning Storage Solutions

If entire storage solutions or individual components thereof are no longer required, any data they contain SHOULD be transferred to other storage solutions. A transitional phase SHOULD be scheduled for this. Afterwards, all payload and configuration data SHOULD be securely deleted. Any references to the decommissioned storage solution SHOULD be removed from any relevant documents.

SYS.1.8.A20 Contingency Planning and Emergency Response for Storage Solutions [Head of IT]

A business continuity plan for the storage solution deployed SHOULD be drawn up. The plan SHOULD include an accurate description of the steps to take in certain emergency situations. Instructions in the form of safeguards and commands that support error analysis and error correction SHOULD be included, as well. In order to remedy errors, appropriate tools SHOULD be used.

Regular drills and tests of the business continuity plan SHOULD be performed. The data generated during the drills and tests (and after an emergency) SHOULD be deleted securely afterwards.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.1.8 *Storage Solutions* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN

THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.1.8.A21 Use of Storage Pools for Client Separation (CI)

Clients SHOULD be assigned storage resources from different storage pools. In so doing, one storage medium SHOULD only be assigned to one pool at a time. The logical hard disks (LUNs) generated from such a pool SHOULD only be assigned to a single client.

SYS.1.8.A22 Use of a Highly Available SAN Solution [Chief Information Security Officer (CISO)] (A)

A highly available SAN solution SHOULD be used. The replication mechanisms used SHOULD meet the availability requirements of the organisation regarding the storage solution. The configuration of the storage solution SHOULD meet the availability requirements, as well. Furthermore, there SHOULD be a test and consolidation system.

SYS.1.8.A23 Use of Encryption for Storage Solutions [Chief Information Security Officer (CISO)] (CI)

All data stored in storage solutions SHOULD be encrypted. The levels at which encryption is to be performed SHOULD be defined (data in motion and data at rest). In so doing, it SHOULD be ensured that the encryption along the transport channel is relevant for replications and backup traffic, as well.

SYS.1.8.A24 Ensuring the Integrity of the SAN Fabric (I)

In order to ensure the integrity of the SAN fabric, protocols with additional security features SHOULD be used. Regarding the following protocols, their security features SHOULD be taken into consideration and corresponding configurations SHOULD be used:

- Diffie Hellman Challenge Handshake Authentication Protocol (DH-CHAP)
- Fibre Channel Authentication Protocol (FCAP)
- Fibre Channel Password Authentication Protocol (FCPAP)

SYS.1.8.A25 Multiple Overwrites of LUN Data (C)

In SAN environments, data SHOULD be deleted by overwriting the related storage segments of a LUN several times.

SYS.1.8.A26 Securing a SAN with Hard Zoning

In order to segment SANs, hard zoning SHOULD be used.

Additional Information

For more information about threats and security safeguards for module SYS.1.8 *Storage Solutions*, see the following publications, among others:

[27040]	ISO/IEC 27040:2015: Information technology - Security techniques - Storage security, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, January 2015
---------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[ISFSY14]	The Standard of Good Practice for Information Security : Area SY1.4 Network Storage Systems, Information Security Forum (ISF), June 2018
-----------	------------------------------------------------------------------------------------------------------------------------------------------

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.1.8 *Storage Solutions*:

- G 0.8 Failure or Disruption of the Power Supply
- G 0.11 Failure or Disruption of Service Providers
- G 0.15 Eavesdropping
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.24 Destruction of Devices or Storage Media
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.40 Denial of Service
- G 0.44 Unauthorised Entry to Premises
- G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0. 8	G 0. 11	G 0. 15	G 0. 16	G 0. 18	G 0. 19	G 0. 20	G 0. 21	G 0. 22	G 0. 23	G 0. 24	G 0. 25	G 0. 26	G 0. 27	G 0. 28	G 0. 29	G 0. 30	G 0. 31	G 0. 32	G 0. 40	G 0. 44	G 0. 45	G 0. 46
SYS.1.8. A1	X			X						X											X		
SYS.1.8. A2			X			X	X			X					X							X	X
SYS.1.8. A3																X		X					
SYS.1.8. A4			X						X	X						X							
SYS.1.8. A5													X	X									
SYS.1.8. A6					X									X	X	X							
SYS.1.8. A7					X									X	X	X							
SYS.1.8. A8					X		X																
SYS.1.8. A9		X			X																		
SYS.1.8. A10					X																		
SYS.1.8. A11											X	X	X										
SYS.1.8. A12						X											X						
SYS.1.8. A13													X	X									

SYS.1.8. A14		X					X	X											
SYS.1.8. A15		X					X	X											
SYS.1.8. A16				X															
SYS.1.8. A17									X	X									
SYS.1.8. A18							X	X			X	X							
SYS.1.8. A19				X															
SYS.1.8. A20										X									X
SYS.1.8. A21		X					X	X											
SYS.1.8. A22									X						X				X
SYS.1.8. A23		X																	
SYS.1.8. A24																			X
SYS.1.8. A25				X															
SYS.1.8. A26		X					X	X											



SYS.2.1: General Client

Description

Introduction

The term “general client” refers to an IT system with any operating system that allows the separation of users. It should be possible to configure at least an administrator and a user environment. Typically, an IT system of this type is networked and used as a client in a client-server network. The IT system can be operated on any platform. For example, this can be a PC with or without a hard drive, a mobile or stationary device, but also a Linux workstation or an Apple Mac. The IT system generally has drives for removable storage media, additional interfaces for data exchange and other peripheral devices.

Objective

The objective of this module is to protect information which is created, read, edited, stored or sent on clients regardless of the operating system they run.

Not in Scope

In general, client systems are operated in an operating system which requires its own security safeguards. For widely used operating systems, separate modules are available which are complemented by the present module. The module *SYS.2.1 General Client* forms the basis for these specific modules. If a specific module exists for a given IT system, that module must be applied in addition to module *SYS.2.1 General Client*. If there is no specific module for the client systems used, the requirements of this module must be adapted in a suitable manner. Security recommendations for mobile devices that cannot be configured freely (such as smartphones or tablets) can generally be found in the layer *SYS.3 Mobile Devices*.

If the client has further interfaces for data exchange (e.g. USB, Bluetooth, LAN or WLAN), these need to be protected in line with the organisation’s security policies as set out in the relevant modules. Information on this can be found in *SYS.3.4 Mobile Storage Media*, *NET.2.4 Near Field Communication* and *NET.2.2 WLAN Usage*.

Threat Landscape

For module *SYS.2.1 General Client*, the following specific threats and vulnerabilities are of particular importance:

Malware

Malware is developed with the goal of executing unwanted and malicious functions on computers. In most cases, it becomes active without the awareness or consent of users. Depending

on its form, malware provides an attacker with comprehensive communication and control channels with an array of functions. Malware can be specifically used to obtain passwords, control IT systems remotely, disable protective software and obtain data, among other things.

Clients are particularly vulnerable: they are operated directly by users and are thus often the entry point for malware. If the users visit infected websites, open e-mails with compromised content from private e-mail accounts or copy malware via local storage media to the client, the malware will spread into the organisation's network via the clients. Central protection mechanisms such as anti-virus protection on the file or e-mail server can thus be bypassed.

Unstructured Organisation of Local Data

Despite regular recommendations to the contrary, many users only save important data locally. For example, data is often stored in local user directories instead of on a central file server. E-mails are often only archived locally, as well. This procedure can lead to the following problems:

- data loss when hardware defects arise
- the inability to access relevant data when a substitute takes over

Even if basic requirements for central storage are observed, however, additional local copies of centrally stored data are often made. This may lead to the following problems:

- wastage of local storage space
- premature deletion of data (or failure to delete data)
- inconsistent versions

Data Loss

Typically, a large amount of data is stored on clients across the entire organisation, the loss of which can have significant impacts on business processes and thus on the entire organisation. When business data is destroyed or corrupted, this can cause delays in business processes and specialised tasks, or even prevent their execution. Overall, the loss of stored data can lead to unproductive time and additional costs of recovery, and especially to long-term consequences such as a loss of trust among customers and partners or a negative public image. In extreme cases, the direct and indirect damage caused by a loss of data can threaten the existence of an organisation.

Hardware Defects Due to Incorrect Operation

As opposed to central IT systems such as servers, client users work directly on their end devices. Through this physical access, they may intentionally or unintentionally damage the client. For example, they may kick IT systems standing on the floor, knock over monitors, trip over cables or pour drinks onto keyboards. It is often not enough to replace hardware only after it proves defective. In the case of a hard drive, for example, it is often not possible to restore the data it contains. Moreover, the IT system will not be available until the repairs are complete. If a mobile device fails while the user is travelling, they will not be able to resume their work until they return.

Software Vulnerabilities or Errors

As a general rule for all types of software, the more complex it is, the more frequently programming or design errors will occur. Software vulnerabilities or errors are understood to involve programming errors that are often (as yet) unknown to the users and constitute a security risk to the system. Almost daily, new vulnerabilities are found in software that has been in use for a long time, but also in new software.

In general, a large number of different applications are installed on clients, which increases the amount of vulnerabilities which may affect the system. In addition, it is much more difficult to update a larger number of (mobile) clients with patches than it is, for example, for a small number of servers.

If software errors are not detected or not immediately rectified, this may have serious consequences. A software vulnerability in frequently used standard software can quickly lead to worldwide security problems for all types of organisations.

Unauthorised Use of IT

The identification and authentication of users is intended to prevent a client from being used in an unauthorised manner. However, IT systems where users are required to identify and authenticate themselves via user IDs and passwords can also be used in an authorised manner if an attacker succeeds in obtaining or guessing access data. If no screen lock is activated, it is possible for the client to be used in an unauthorised manner, even during a short absence.

Provision of Unnecessary Operating System Components and Applications

When installing an operating system, there is generally the possibility to remove optional software. Software is regularly installed and tested during live operation, as well. With every use, the computing and storage load on a client continuously increases, as does the probability of finding vulnerabilities therein. Software that is not required is often not subject to regular patch management, which means that even known vulnerabilities are not rectified promptly. This enables attackers to make use of vulnerabilities that have been known for a long time.

Eavesdropping on Rooms Using Microphones and Cameras

Many clients are equipped with a microphone and camera. This also includes intelligent personal assistants (IPAs or voice assistants), which constantly listen to their environment and carry out certain functions (such as playing music, calling contacts, controlling lighting or changing the room climate) according to a device-dependent code word. These microphones and cameras can be used by anyone who has corresponding access rights, and also by external parties in the case of networked systems. If these rights are not carefully assigned, unauthorised persons can abuse the microphone or camera to eavesdrop on rooms or record meetings unnoticed via the internet. If calls (e.g. from IPAs) are transmitted to third parties via data connections, they may be intercepted. The recorded calls could also be stored and processed by the IPA operators.

Requirements

The specific requirements of module *SYS.2.1 General Client* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according

to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User, Building Services

Basic Requirements

For module SYS.2.1 *General Client*, the following requirements **MUST** be implemented as a matter of priority:

SYS.2.1.A1 User Authentication

In order to use the client, the users **MUST** be authenticated by the IT system. If the users are to use passwords for this, secure passwords **MUST** be used. The passwords **MUST** comply with the organisation's password policy (see ORP.4 *Identity and Access Management*).

SYS.2.1.A2 Separation of Roles

The client **MUST** be configured in such a way that normal activities are not carried out with administrator rights. Only administrators **MAY** obtain administrator rights. Only administrators **MAY** change the system configuration, install or remove applications or modify or delete system files. Users **MAY ONLY** have read access to system files.

Procedures, framework conditions and requirements for administrative tasks, as well as the separation of duties between the different roles of the IT system users, **SHOULD** be established in a user and administration concept.

SYS.2.1.A3 Activation of Automatic Update Mechanisms

Automatic update mechanisms **MUST** be activated unless other mechanisms (such as regular manual maintenance or a central software distribution system) are used for updates. If a time interval can be specified for auto-update mechanisms, there **SHOULD** be an automatic search for updates at least daily and they **SHOULD** be installed if found.

SYS.2.1.A4 Regular Backups

In order to avoid irretrievable losses of data, regular backups of the data **MUST** be made. In most computer systems, the backup process can be largely automated. Rules **MUST** be defined to specify which locally stored data is backed up by whom and at what time. At minimum, the data that cannot be derived from other information **MUST** be backed up regularly. Clients **MUST** also be included in the organisation's backup concept. For confidential and outsourced backups, the backed up data **SHOULD** be stored in encrypted form. A separate decision **SHOULD** be made as to whether the software used needs to be included in regular backups. Tests **MUST** be performed regularly to determine if the backup process functions as desired, and in particular if the data backed up can also be restored without any problems. The users **SHOULD** be informed of the rules specifying how backups are to be made and by whom.

SYS.2.1.A5 Screen Locking [User]

A screen lock **MUST** be used to prevent unauthorised persons from accessing the activated clients. It **SHOULD** be possible for the user to activate the screen lock manually. In addition, the

screen lock should be automatically initiated after a predefined period of inactivity. It MUST be ensured that the screen lock can only be deactivated after successful user authentication.

SYS.2.1.A6 Use of Anti-Virus Programs

Depending on the installed operating system and other existing protection mechanisms of the client, it MUST be checked whether virus protection programs are to be used. Concrete statements as to whether virus protection is required can usually be found in the operating system modules of the IT-Grundschutz compendium. The corresponding signatures of a virus protection program MUST be updated at regular intervals. In addition to real-time and on-demand scans, it MUST also be possible to scan compromised and encrypted data for malware with the solution chosen.

The virus protection programs on the clients MUST be configured so that the users cannot make any security-relevant changes to the settings or deactivate them.

SYS.2.1.A7 Logging

It MUST be decided which minimum information is to be logged on clients, how long the log data is kept and who is allowed to view the log data under which conditions. As a matter of principle, all security-relevant system events MUST be logged.

SYS.2.1.A8 Protection of the Boot Process

The start-up procedure of the IT system (boot process) MUST be protected against manipulation. It MUST be defined which media can be used to boot the system. A decision SHOULD be made as to whether and how the boot process is to be protected cryptographically. It MUST be ensured that only administrators can boot the clients from anything other than the default drive, or from an external storage medium. Only administrators MAY boot from integrated optical or external storage media. The ability to change the configuration settings of the boot process firmware MUST be restricted to users with administrative rights. All unused functions in the firmware MUST be disabled.

Standard Requirements

For module SYS.2.1 *General Client*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.2.1.A9 Defining a Security Policy for Clients

On the basis of the general security policy of the organisation, the requirements for general clients SHOULD be specified. The policy SHOULD be known to all users and all persons involved in the procurement and operation of the clients, and must form the foundation of their work. The implementation of the contents required in the policy SHOULD be checked at regular intervals. The results SHOULD be appropriately documented.

SYS.2.1.A10 Planning the Use of Clients

For the secure operation of clients, it SHOULD be planned in advance where and how the clients are to be used. Planning SHOULD address not only aspects that are associated with security in a traditional sense, but also normal operational aspects that entail requirements in the area of security. In addition to client-type-specific requirement profiles, specifications regarding authentication and user administration SHOULD be defined. All decisions made in the

planning phase SHOULD be documented in such a way that they can be understood at any given future point in time.

SYS.2.1.A11 Procurement of Clients

Before clients are procured, a requirements list SHOULD be drawn up that can be used to evaluate the products available on the market. The relevant manufacturer SHOULD be able to promptly provide patches for vulnerabilities throughout the planned duration of use. The systems to be procured SHOULD have a firmware configuration interface for UEFI SecureBoot and for the TPM (if available), which allows for control by the owner (organisation) and thereby enables the self-managed operation of SecureBoot and the TPM.

SYS.2.1.A12 Checking Software for Compatibility

Before procuring any software, the software's compatibility with the operating system used in the present configuration SHOULD be checked; this compatibility check should be included in the approval procedure of the software. If no binding information on compatibility is available from the manufacturer, the compatibility SHOULD be tested in a test environment. Before an intended hardware change or an operating system migration, the driver software for all relevant components SHOULD also be checked for compatibility with the operating system.

SYS.2.1.A13 Access to Runtime Environments with Unmonitored Code Execution

Access to runtime environments with unmonitored code execution (e.g. storage areas specifically secured by the operating system, firmware areas) SHOULD only be possible for users with administrative rights. The corresponding settings in the BIOS or the UEFI firmware SHOULD be protected against changes by a password. If control over the functions is delegated to the operating system, only users with administrative authorisations SHOULD be able to control the functions there.

SYS.2.1.A14 Updates and Patches for Firmware, Operating Systems and Applications

Administrators SHOULD inform themselves regularly about vulnerabilities which have recently become known. The identified vulnerabilities SHOULD be rectified as soon as possible. As a matter of principle, it SHOULD be ensured that patches and updates are only obtained from trusted sources. If necessary, the relevant applications or the operating system SHOULD be restarted following the update.

When no corresponding patches are available, other suitable safeguards to protect the IT system SHOULD be taken depending on the severity of the vulnerabilities.

SYS.2.1.A15 Secure Installation and Configuration of Clients

It SHOULD be specified which operating system components, specialised applications and other tools are to be installed. The installation and configuration of the IT systems SHOULD only be performed by authorised persons (administrators or service providers bound by contract) according to a defined installation process. All installation and configuration steps SHOULD be documented in such a way that the installation and configuration can be understood and repeated by a qualified third party based on the documentation (see also SYS.2.1.A40 *Operational Documentation*).

The basic settings of clients SHOULD be checked and, where necessary, adapted to the specifications of the security policy. The client SHOULD only be connected to the Internet after the installation and configuration have been completed.

SYS.2.1.A16 Deactivation and Removal of Unnecessary Components and IDs

The components of the firmware, operating system, applications and other tools that are installed and activated on the clients SHOULD be checked after installation. Unnecessary modules, programs, services, user IDs and interfaces SHOULD be deactivated or removed. In addition, unnecessary runtime environments, interpreter languages and compilers SHOULD be removed. Components that are not required as a result but have a fixed connection to the IT system SHOULD be disabled. Unnecessary components in the firmware (e.g. anti-theft protection, remote maintenance) SHOULD also be switched off. The reactivation of these components SHOULD be prevented. The decisions made SHOULD be documented in such a way that it can be understood which configuration and software equipment was chosen for the IT systems.

SYS.2.1.A17 Approval for Use

Before the client is connected to a production network and used in production operations, it SHOULD be approved for use. This SHOULD be documented. Before they are approved for use, the installation and configuration documentation and the functionality of the IT systems SHOULD be checked in a test. This SHOULD be performed by a department authorised for this purpose in the organisation.

SYS.2.1.A18 Use of TLS [User]

Communication links SHOULD be protected by encryption whenever possible. Users SHOULD ensure that SSL/TLS is used for websites.

The IT Operation Department SHOULD ensure that the client products used support secure versions of TLS. The clients SHOULD use cryptographic algorithms and key lengths that conform to the current state of the art and meet the security requirements of the organisation.

New certificates SHOULD only be used after checking the fingerprint. The validation of certificates SHOULD be enabled in application programs such as browsers and e-mail clients. Session renegotiation and TLS compression SHOULD be deactivated.

SYS.2.1.A19 Restrictive Granting of Access Rights

The available scope of functions of the IT system SHOULD be restricted for individual users or user groups so that they only have the rights and function access they require to fulfil their tasks. Access authorisations SHOULD be granted as restrictively as possible. It SHOULD be checked at regular intervals whether the authorisations (for system directories and files in particular) correspond to the specifications of the security policy. If possible, only system administrators SHOULD have access to system files. The group of administrators with the authorisations required to access these files SHOULD be kept as small as possible. Directories SHOULD also provide no more than the required privileges for users.

SYS.2.1.A20 Protection of Administration Interfaces

Depending on whether clients are administrated locally, via the network or via central network-based tools, adequate security precautions SHOULD be taken. The methods applied for administration SHOULD be specified in the security policy and administration SHOULD only be performed in accordance with the security policy. Administration via the network SHOULD be performed via secure protocols.

SYS.2.1.A21 Preventing Unauthorised Use of Computer Microphones and Cameras

Access to the microphone and camera of a client SHOULD only be available to the users themselves while they are working locally on the IT system. If an existing microphone or camera is

not used and its misuse is to be prevented, it SHOULD be switched off, covered (camera only), deactivated or physically disconnected from the device whenever possible. Rules SHOULD be specified on how cameras and microphones in clients are to be used and how the rights are to be assigned.

SYS.2.1.A22 Logging Out After Completing Tasks [User]

All users SHOULD be obliged to log out of the IT system or application after completing their tasks, particularly when a system is used by several users. If a user assumes that only a short interruption of their work is required, they SHOULD activate the screen lock instead of logging off. If technically possible, the screen lock SHOULD be activated (or the user logged off) automatically after a longer period of inactivity.

SYS.2.1.A23 Use of Client-Server Services

If possible, dedicated server services for information exchange SHOULD be used and direct connections between clients avoided. If this is not possible, it SHOULD be specified which client-to-client services (previously often referred to as "peer-to-peer") may be used and which information may be exchanged through them. If necessary, the users SHOULD be trained in the use of such services. Direct connections between clients SHOULD be restricted to the LAN. Auto-discovery protocols SHOULD be restricted to those required.

SYS.2.1.A24 Handling Removable Media During System Operations

Installation of uncontrolled software or unauthorised copying of data via storage media or interfaces to clients SHOULD be prevented. Interfaces to other networks SHOULD ONLY be possible in a restricted manner. Access to data or removable media from untrusted sources from the clients SHOULD be prevented in general.

SYS.2.1.A25 Policy for Secure IT Use [User]

A policy SHOULD be drawn up for all employees which transparently describes which framework conditions must be observed during IT use and which security safeguards must be implemented. The policy SHOULD cover the following aspects:

- security objectives of the organisation
- important terms
- tasks and roles with respect to information security
- contact persons for questions regarding information security
- security safeguards to be implemented and observed by the employees

The policy SHOULD be brought to the attention of all users. Every new user SHOULD confirm that they have read the policy before being allowed to use the information technology. After more comprehensive changes are made to the policy (or after two years at the latest), reconfirmation SHOULD be required.

SYS.2.1.A26 Protection of Applications

To make it more difficult to exploit vulnerabilities, ASLR and DEP/NX SHOULD be activated in the kernel and used by the applications. Security functions of the kernel and the standard libraries (such as heap and stack protection) SHOULD NOT be deactivated.

SYS.2.1.A27 Orderly Decommissioning of Clients

When decommissioning a client, it SHOULD be ensured that no important data that might still be present on the storage media is lost and no sensitive data remains. There SHOULD be an overview of the data stored at each location on the IT systems. A checklist which can be completed when decommissioning an IT system SHOULD be created. This checklist SHOULD, at minimum, include aspects of backing up data that is still needed and the subsequent secure deletion of all data.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.2.1 *General Client* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.2.1.A28 Encryption of Clients (C)

If confidential information is stored on the clients, the sensitive files and select areas of the file system – or better yet, the entire hard drive – SHOULD be encrypted. A separate concept SHOULD be drawn up for this and the configuration details SHOULD be documented in a particularly thorough manner because the data on the encrypted file systems may be lost completely in the event of problems. In this context, the following aspects SHOULD be regulated: authentication (e.g. passwords, PINs, tokens), storage of the recovery information, drives to be encrypted, write privileges on unencrypted storage media and how to ensure that recovery information is only accessible to authorised persons. Encrypted files, partitions and storage media SHOULD also be backed up at regular intervals. The key material used MUST NOT be stored as plain text on the clients.

The users SHOULD be informed of how to respond if they lose authentication resources.

SYS.2.1.A29 System Monitoring (A)

The clients SHOULD be integrated into a suitable system monitoring concept that continuously monitors the system status and the functionality of the clients while also reporting error conditions and exceeded thresholds to the operating personnel.

SYS.2.1.A30 Setting Up a Reference Installation for Clients (CIA)

A reference installation SHOULD be set up for clients in which the basic configuration and all configuration changes, updates and patches can be tested before installing them on the users' clients. This reference installation SHOULD also be used to simplify the installation of new clients or to continue the use of existing clients by copying the respective preconfigured installation to the clients to be installed ("cloning") in an appropriate way. Checklists SHOULD be drawn up for typical and frequently recurring test cases which can be completed during testing. In addition, all tests SHOULD be documented in such a way that they can be reconstructed at a later point in time.

SYS.2.1.A31 Configuring Local Packet Filters (CIA)

In addition to the central security gateways used, local packet filters SHOULD be used on all computers. A whitelist strategy SHOULD be chosen for packet filter implementation.

SYS.2.1.A32 Use of Additional Safeguards to Protect Against Exploits (CIA)

Additional safeguards SHOULD be implemented on the IT system as explicit protection against exploits of system gaps. If it is not possible to fulfil necessary security safeguards by means of built-in utilities, suitable security products SHOULD also be used. If it is not possible to implement corresponding safeguards by means of built-in utilities or a suitable security product, other suitable (generally organisational) security safeguards SHOULD be implemented.

SYS.2.1.A33 Application Whitelisting (CIA)

By means of application whitelisting, it SHOULD be ensured that only authorised programs and scripts are executed. The rules SHOULD be set as restrictively as possible. If explicit specification of paths and hashes is not possible, certificate-based or path rules SHOULD be used as an alternative.

SYS.2.1.A34 Use of Application Isolation (CIA)

Applications used to edit external data SHOULD only be operated in a process environment that is isolated from the operating system.

SYS.2.1.A35 Active Administration of Root Certificates (CI)

As part of the procurement and installation of the clients, it SHOULD be documented which root certificates are required for their operation. Only the previously documented root certificates required for operation SHOULD be present on the client. Regular checks SHOULD be made as to whether the existing root certificates still comply with the organisation's requirements. All certificate stores available on the IT system (e.g. UEFI certificate stores, certificate stores of web browsers) SHOULD be included in these checks.

SYS.2.1.A36 Self-Managed Use of SecureBoot and TPM (CI)

On UEFI-compatible systems, the bootloader, kernel and all required firmware components SHOULD be signed by self-controlling key material, and any key material that is not required SHOULD be removed. If the TPM is not required, it SHOULD be deactivated.

SYS.2.1.A37 Protection Against Unauthorised Logins (CIA)

To prevent access to the system using compromised login information, multi-factor authentication SHOULD be used.

SYS.2.1.A38 Integration into Contingency Planning (A)

The clients SHOULD be taken into account in the business continuity management process. The clients must be prioritised for restoration of service according to the business processes for which they are needed. At minimum, suitable business continuity safeguards SHOULD be implemented by drawing up recovery plans, generating boot media for system recovery and securely storing passwords and cryptographic keys.

SYS.2.1.A39 Uninterruptible and Stable Power Supply [Building Services] (A)

In case of higher requirements regarding the availability of stationary clients, these SHOULD be connected to an uninterruptible power supply (UPS). The UPS SHOULD be dimensioned sufficiently in terms of its output power and backup time. If changes have been made to the consumers, it SHOULD be checked again whether the backup time is sufficient. Overvoltage protection SHOULD be available for both the UPS devices and the clients.

The actual capacity of the battery (that is, the backup time the UPS can provide) SHOULD be tested at regular intervals. The UPS SHOULD be maintained at regular intervals.

SYS.2.1.A40 Operational Documentation

The execution of operational tasks on clients SHOULD be documented in a traceable manner (in terms of what, when and by whom), especially if this affects groups of clients. Based on the documentation, changes to the configuration in particular SHOULD be transparent; security-relevant tasks (for example, who is authorised to install new hard drives) SHOULD also be documented. Everything that can be documented automatically SHOULD be documented automatically. The documentation SHOULD be protected against unauthorised access and loss.

SYS.2.1.A41 Preventing the Local Hard Drive from Becoming Overloaded (A)

Consideration SHOULD be given to configuring quotas. As an alternative, mechanisms of the file or operating system in question SHOULD be used that warn the users or only grant write privileges to the system administrator if the hard drive capacity reaches a specific level.

Additional Information

For more information about threats and security safeguards for module SYS.2.1 *General Client*, see the following publications, among others:

[ISiClient]	Whitepaper Absicherung eines PC-Clients (ISi-Client) [White Paper Securing a PC Client (ISi-Client): Federal Office for Information Security (BSI), 2011, https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Client/client_node.html , last accessed on 05.09.2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 05.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.2.1 *General Client*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.36 Identity Theft

G 0.39 Malware

G 0.40 Denial of Service

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

G 0.43 Attack with Specially Crafted Messages

Elementary Threats Requirements	G 0.14	G 0.15	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.26	G 0.28	G 0.30	G 0.31	G 0.36	G 0.39	G 0.40	G 0.45	G 0.46	G 0.43
SYS.2.1.A1	X		X			X	X						X					
SYS.2.1.A2					X	X					X	X	X					X
SYS.2.1.A3				X				X	X	X								
SYS.2.1.A4																X	X	
SYS.2.1.A5			X			X	X				X		X					
SYS.2.1.A6					X	X			X					X	X			
SYS.2.1.A7							X		X									
SYS.2.1.A8					X	X					X	X						X
SYS.2.1.A9			X									X					X	
SYS.2.1.A10						X	X					X					X	
SYS.2.1.A11								X					X					
SYS.2.1.A12								X	X						X			
SYS.2.1.A13					X						X							
SYS.2.1.A14					X				X	X								
SYS.2.1.A15					X	X	X				X				X		X	
SYS.2.1.A16			X				X			X	X				X		X	
SYS.2.1.A17									X	X								
SYS.2.1.A18		X	X														X	X
SYS.2.1.A19			X			X					X					X	X	
SYS.2.1.A20		X			X						X							
SYS.2.1.A21	X	X	X															

SYS.2.1.A22	X		X			X				X		X					
SYS.2.1.A23				X	X		X				X			X	X		
SYS.2.1.A24	X										X		X				
SYS.2.1.A25											X						
SYS.2.1.A26				X		X			X								
SYS.2.1.A27	X		X														
SYS.2.1.A28	X	X	X														X
SYS.2.1.A29				X			X	X						X			
SYS.2.1.A30				X				X			X						
SYS.2.1.A31						X				X				X			
SYS.2.1.A32			X	X	X	X			X	X			X	X	X	X	
SYS.2.1.A33				X							X		X				X
SYS.2.1.A34				X							X		X				X
SYS.2.1.A35	X	X	X											X			
SYS.2.1.A36	X		X	X	X		X				X						
SYS.2.1.A37	X		X				X				X		X	X		X	X
SYS.2.1.A38							X	X									
SYS.2.1.A39							X	X			X						
SYS.2.1.A40				X			X										
SYS.2.1.A41							X				X					X	



SYS.2.2.2: Windows 8.1 Clients

Description

Introduction

In Windows 8, Microsoft has presented a further development of its client operating system Windows and the features and components introduced with it. The new feature of Windows 8 is its user interface, which is tailored to the use of portable devices with touchscreens. This involves a new operating concept for applications. Microsoft has also provided a class of mobile applications ("apps") to be used in Windows 8 in addition to the conventional desktop applications. These apps are primarily designed to be controlled by means of touch. In addition, they can perform display functions as "tiles" on the screen. Some applications, above all the version of Internet Explorer delivered with Windows 8, are available in two variants for Windows 8. Since the introduction of Windows 8, Microsoft has made some improvements and integrated them into the operating system, which has thus been assigned the version number 8.1.

Objective

The objective of this module is to protect information that is processed in Windows 8.1, including by corresponding clients.

Not in Scope

This module must be applied to all target objects that run the Windows 8.1 operating system. Whenever the security requirements and threats only apply to Windows 8, this is explicitly indicated in the texts. The requirements of module SYS.2.1 *General Client* must also be met. The present module specifies and complements requirements specific to Windows 8.1. For application programs used on Windows clients, the requirements of the corresponding modules must be fulfilled – for example, APP.1.1 *Office Products* or APP.1.2 *Web Browsers*. When used in a Windows domain, the requirements of the corresponding modules, such as APP.2.2 *Active Directory*, must be fulfilled.

Threat Landscape

For module SYS.2.2.2 *Windows 8.1 Clients*, the following specific threats and vulnerabilities are of particular importance:

Malware Designed for Windows

Malware provides an attacker with a wide range of communication and control capabilities and has a variety of functions. Among other purposes, malware may be used to obtain specific passwords, control systems remotely, disable protective software and collect data without authorisation. A removable medium could be manipulated to install and execute malware when

it is inserted or connected. The most serious damage that can be caused by malware is the loss or corruption of information or applications. However, the reputational and financial damage that may result from malware may also be significant. Due to its widespread use, Windows is a primary target that is highly exposed to numerous attackers and many different types of malware attacks.

Software Vulnerabilities or Errors

Windows 8.1, including the numerous applications that come with it, is a very complex software product. If software errors in this product are detected too late, the crashes or errors that occur in using it may have far-reaching consequences (e.g. incorrect calculation results, incorrect decisions at the top management level and delays in business processes). Software vulnerabilities or errors may result in serious vulnerabilities in individual applications, the entire IT system or even all the IT systems connected to it. Vulnerabilities in Windows may be exploited by attackers to inject malware, obtain data without authorisation or perform manipulations.

Integrated Cloud Functions

Windows 8.1 includes numerous features that are used to store and synchronise data in the cloud services of Microsoft. Here, there is the risk that this will result in the unwitting (or at least careless) use of cloud services in connection with sensitive or personal data. At the same time, violations of data protection laws are also possible if the data is stored with third parties, especially abroad. If a user logs into a new device using an already activated Microsoft account, the Microsoft cloud services used by the user will be set up automatically on the device. This way, company data may accidentally be synchronised to employees' private devices. As another example, Windows 8 offers the default option to back up the BitLocker recovery key directly in the cloud via one's Microsoft account. This amounts to handing critical cryptographic secrets over to a third party.

Impairment of Software Features Due to Compatibility Issues

Software that ran successfully on previous Windows versions will not necessarily work with a current version of the operating system. Possible reasons for this may include new security features or operating system properties, as well as the discontinuation of functions or services. As a result, use of the software may be limited or completely impossible. For new Windows versions, activating new security features (for example) may result in compatibility issues. Examples of this include User Account Control (UAC) or, in 64-bit versions of the operation system, Kernel Patch Protection, and the necessity of signed drivers. Meanwhile, some functions have also been discontinued in newer Windows versions. One example includes the discontinuation of the GINA login component in newer Windows versions, which was used by several fingerprint readers, for example.

Incorrect Administration or Use of Devices and Systems

Windows operating systems are complex systems whose security is determined primarily by the parameters set. In particular, incorrect configurations of components may impair security and result in malfunctions occurring or the IT system being compromised. In general, each interface on an IT system not only provides the opportunity to use certain services of the IT system in an authorised manner, but also carries the risk of the IT system being accessed via these interfaces without authorisation. If, for example, user IDs and associated passwords can be obtained due to the incorrect configuration of Windows' own authentication mechanisms, it is possible that the applications or IT systems protected will be used in an unauthorised manner.

Incorrect or improper use of devices, systems and applications may also jeopardise security in Windows, especially if existing security safeguards are ignored or bypassed. Security incidents may occur when access rights are granted too generously, passwords are easy to guess, storage media containing backup copies are inadequately protected or workstations are not locked during temporary periods of absence. Another possible consequence of the incorrect operation of Windows systems or applications involves the accidental deletion or modification of data. Here, it is also possible that confidential information will be published – for example, if access rights are used improperly.

Requirements

The specific requirements of module *SYS.2.2.2 Windows 8.1 Clients* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User

Basic Requirements

For module *SYS.2.2.2 Windows 8.1 Clients*, the following requirements **MUST** be implemented as a matter of priority:

SYS.2.2.2.A1 Selection of a Suitable Windows 8.1 Version

The scope of functions of a Windows version **MUST** be checked for its applicability prior to procurement and an appropriate version **MUST** be selected. Preferably, 64-bit versions including advanced security features **SHOULD** be used.

SYS.2.2.2.A2 Definition of a Login Process

Depending on the security requirements, it **MUST** be decided whether other mechanisms such as PINs are to be allowed in addition to the conventional login process using a password. This **MUST** be set accordingly on all clients.

SYS.2.2.2.A3 Use of Anti-Virus Programs

Unless equivalent or higher-order safeguards have been implemented to protect the IT system from malware, an anti-virus program must be used on Windows 8 clients.

Standard Requirements

For module *SYS.2.2.2 Windows 8.1 Clients*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

SYS.2.2.2.A4 Procurement of Windows 8.1

The requirements according to the Windows Hardware Certification Requirements SHOULD be taken into consideration when procuring Windows 8.1 or the corresponding hardware for the Windows 8.1 system. Furthermore, the systems to be procured SHOULD have a firmware configuration interface for UEFI SecureBoot and for the TPM (if applicable), which allows for control by the owner. The procurement process for Windows 8.1 SHOULD include the selection of a suitable licence model.

SYS.2.2.2.A5 Local Security Policies

All security-relevant settings SHOULD be configured, tested and checked regularly as needed with the help of security policies. All applications and components that are not needed SHOULD be disabled using security policies. The distribution of the security settings to several Windows 8.1 clients SHOULD be performed in accordance with the circumstances of the organisation.

SYS.2.2.2.A6 File and Sharing Authorisations

To enable uniform and restrictive assignment of rights, there SHOULD be an authorisation and access concept for Windows that defines appropriate file and directory authorisations according to the need-to-know principle for content on Windows 8.1 clients.

In addition to authorisations on the local file system, the authorisation and access concept SHOULD consider the access rights for shared directories in network access. The authorisations of the files and directories SHOULD be checked, particularly on computers that have been upgraded from older operating system versions.

SYS.2.2.2.A7 Use of Windows User Account Control (UAC)

In order to support restrictive rights assignment, User Account Control (UAC) SHOULD be enabled. For standard users, it SHOULD be defined that password prompts will be rejected automatically for higher rights. For administrator accounts, a balance between user-friendliness and security SHOULD be achieved when configuring UAC. This decision SHOULD be documented and the corresponding settings SHOULD be configured. It SHOULD be checked regularly whether the necessity still exists and the rights SHOULD be adapted or withdrawn accordingly.

SYS.2.2.2.A8 Use of the Homegroup Feature [User]

Clients SHOULD not offer any services such as file or printer sharing. A security policy (GPO) with the setting “Prevent the computer from becoming a member in a homegroup” SHOULD apply to all clients. If the feature is being used for internal reasons, the users SHOULD be trained regarding the handling of the homegroup.

SYS.2.2.2.A9 Data Protection and Data Economy in Windows 8.1 Clients [User]

If Microsoft accounts are created for the users, only the personal information absolutely required SHOULD be entered. The SmartScreen feature, which checks files and web content downloaded from the Internet and transmits personal data to Microsoft in the process under certain circumstances, SHOULD be disabled. Before an application or app is approved for use within the organisation, the data it automatically sends to the Microsoft cloud SHOULD be checked carefully. Applications SHOULD be configured to prevent the transmission of such data. Apps that involve undesired or unnecessarily comprehensive data transmissions to third parties SHOULD not be used.

SYS.2.2.2.A10 Integration of Online Accounts into the Operating System

Logging into the IT system and the domain SHOULD only be possible using an account of a self-operated directory service (e.g. Active Directory). The ability to log in locally SHOULD be reserved for administrators. When using online accounts to log in (e.g. Microsoft accounts or accounts from other providers of identity management services), the sufficient security of the provider and its compliance with data protection SHOULD be ensured.

SYS.2.2.2.A11 Configuration of Synchronisation Mechanisms in Windows 8.1

The synchronisation of user data with Microsoft cloud services SHOULD be disabled completely.

SYS.2.2.2.A12 Central Authentication in Windows Networks

In purely Windows-based networks, only Kerberos SHOULD be used for central SSO (single sign-on) authentication. A group policy SHOULD prevent the use of older protocols. The PPL (Protected Process Light) protection of the local security authority (LSA) SHOULD be activated. Storage of the LAN Manager hash values when changing passwords SHOULD be disabled based on a group policy. The monitoring settings SHOULD be aligned carefully with the requirements of the information domain together with the server components of DirectAccess. Client-side logging SHOULD be ensured.

SYS.2.2.2.A13 Connecting Windows 8.1 to App Stores

The option of installing apps from the Microsoft Store SHOULD be disabled unless it is required.

Requirements in Case of Increased Protection Needs

Generic suggestions for module *SYS.2.2.2 Windows 8.1 Clients* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.2.2.2.A14 Application Control Using Software Restriction Policies and AppLocker (CIA)

Applications in paths for which users have write rights SHOULD be prevented from being executed by software restriction policies (SRP) or AppLocker. The administration of AppLocker and SRP GPOs in a domain-based network SHOULD be performed in a centralised manner with the help of group policy objects for each user/user group.

AppLocker SHOULD be used in a whitelist approach. Everything that is not explicitly allowed SHOULD be forbidden. Rules based on the application signatures of defined publishers SHOULD be preferred when using AppLocker. Attempted violations of the rules SHOULD be logged and evaluated appropriately.

For clients with particularly high security requirements, AppLocker SHOULD prevent the execution of any applications not approved (instead of merely logging them).

The SRP and AppLocker rules SHOULD be tested on a test system or by means of operation in the monitoring mode before being used on a production system.

SYS.2.2.2.A15 File System Encryption Using EFS (CI)

In case of increased protection needs, the file system SHOULD be encrypted. If the Encrypting File System (EFS) is used in this regard, a complex password SHOULD be used to protect the data encrypted using EFS. The files encrypted with EFS SHOULD also be protected by restrictive access rights. Instead of the administrator account, a dedicated account SHOULD be the recovery agent. The private key of this account SHOULD be outsourced to an external storage medium, stored securely and removed from the system. In so doing, backups of all private keys SHOULD be created. When using EFS with local user accounts, the registry encryption by means of syskey SHOULD be used. When using EFS, the users SHOULD be trained regarding the proper handling of EFS.

SYS.2.2.2.A16 Use of Windows PowerShell (CIA)

If Windows PowerShell (WPS) is not required, it SHOULD be uninstalled. In Windows 8.1, the PowerShell script environment may only be removed by uninstalling the .NET framework, as well. Alternatively, only the administrator groups (local and domain) SHOULD be permitted to execute the WPS files. The process of logging write- and read-only access to the Windows PowerShell profile SHOULD be enabled and it SHOULD be ensured that the logs are checked regularly. The execution of Windows PowerShell scripts SHOULD be restricted with the command “Set-Execution Policy AllSigned” in order to at least prevent any accidental execution of scripts without a signature.

SYS.2.2.2.A17 Secure Use of the Maintenance Centre (CIA)

The security policy SHOULD define how users are to use the maintenance centre. The settings for “Call up latest troubleshooting from the Windows Online Service for troubleshooting”, “Send error reports”, “Send data on computer configuration at regular intervals to Microsoft”, “Windows backup”, “Program for user-friendliness” and “Troubleshooting – other settings” SHOULD be deactivated in Windows 8.1.

SYS.2.2.2.A18 Activation of the Last Access Time Stamp (A)

When creating a security concept for an IT system using Windows 8.1, it SHOULD be determined whether the last access time stamp is to be enabled to facilitate the analysis of misuse of the system. In so doing, the performance aspects in particular SHOULD be taken into consideration.

SYS.2.2.2.A19 Use of Login Information Management (C)

A policy SHOULD define whether access may be stored in the so-called “vault”. If not, doing so SHOULD be technically impossible.

SYS.2.2.2.A20 Security During Remote Access Using RDP (CIA)

The effects on the configuration of the local firewall SHOULD be taken into account when planning the remote assistance procedures. The group of users authorised for remote desktop access SHOULD be specified in the policy and by assigning the corresponding user rights. Remote assistance SHOULD only be provided after explicit invitation via EasyConnect or on the basis of an invitation file. When storing an invitation in a file, the file SHOULD be protected by a password. In every case, the user currently logged in SHOULD have to agree explicitly to starting a session. The maximum period of validity of the invitation SHOULD have a reasonable length. Strong encryption SHOULD also be used (128-bit, “highest level” setting). Furthermore, automatic password logins SHOULD be disabled. It SHOULD be checked whether diversions of the cache, printer, file deposition, and Smartcard connections are necessary; otherwise,

these SHOULD be disabled. If the use of the remote control mechanisms is not planned, they SHOULD be disabled completely.

SYS.2.2.2.A21 Use of File and Registry Virtualisation (CI)

It SHOULD be checked whether the operation of legacy applications requiring writing rights to critical system folders or registry keys or having to be executed with administrator rights is still required. If this is applicable, a strategy SHOULD be developed in order to switch from the still required legacy applications to secure alternatives. Until the legacy applications are replaced by secure alternatives, the use of the Windows technologies for file virtualisation and registry virtualisation for the security purposes SHOULD be considered. In addition, the registry virtualisation SHOULD only have access to the necessary registry keys.

Additional Information

For more information about threats and security safeguards for module *SYS.2.2.2 Windows 8.1 Clients*, see the following publications, among others:

[MicSAO]	Security Auditing Overview: Microsoft, July 2013, https://technet.microsoft.com/en-us/library/dn319078.aspx , last accessed on 06.09.2018
[MicSE]	List of security events on Windows 8 and Windows Server 2012: Microsoft, https://www.microsoft.com/en-us/download/confirmation.aspx?id=50034 , last accessed on 06.09.2018
[WIN8]	Information on the deployment, provision, and management of Windows 8.1: Microsoft, https://technet.microsoft.com/de-de/windows/windows-8.aspx , last accessed on 06.09.2018
[WINLSA]	Configuring Additional LSA Protection: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection , last accessed on 06.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module *SYS.2.2.2 Windows 8.1 Clients*:

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.1 6	G 0.1 7	G 0.1 8	G 0.1 9	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 5	G 0.2 8	G 0.2 9	G 0.3 0	G 0.3 1	G 0.3 2	G 0.3 6	G 0.3 9	G 0.4 5	G 0.4 6
SYS.2.2.2.A1						X			X	X	X	X					
SYS.2.2.2.A2	X			X		X	X			X	X		X				X
SYS.2.2.2.A3				X						X			X		X	X	X
SYS.2.2.2.A4			X														
SYS.2.2.2.A5				X		X				X	X	X			X		X
SYS.2.2.2.A6	X	X	X	X	X					X	X		X				X
SYS.2.2.2.A7						X						X					X
SYS.2.2.2.A8				X							X					X	
SYS.2.2.2.A9				X		X							X	X	X		X
SYS.2.2.2.A10	X		X	X		X		X		X	X	X				X	
SYS.2.2.2.A11	X		X	X		X		X		X	X	X				X	
SYS.2.2.2.A12			X	X													X
SYS.2.2.2.A13				X		X							X	X	X		X
SYS.2.2.2.A14				X		X							X	X	X		X
SYS.2.2.2.A15				X													X
SYS.2.2.2.A16						X					X	X					
SYS.2.2.2.A17												X					

SYS.2.2.2.A1 8			X			X						X				
SYS.2.2.2.A1 9	X											X				
SYS.2.2.2.A2 0				X							X	X	X			X
SYS.2.2.2.A2 1						X						X				X



SYS.2.2.3: Windows 10 Clients

Description

Introduction

In Windows 10, Microsoft has adapted its Windows client operating system to a new corporate strategy. The changes specifically involve the design philosophy of the operating system, which has moved away from the “local operating system” principle towards a service (“Windows as a service”). In addition to the previous operating system functions, this service includes applications that go beyond said functions (specifically cloud-based applications) and, as a consequence, it depends on a close connection to the server infrastructure of the manufacturer. Here, the deeply integral exchange of data between clients and the manufacturer's infrastructure (some of which cannot be influenced), as well as the increasing outsourcing of security-critical core parts of the Windows infrastructure (such as authentication) into the cloud are important new aspects that definitely have to be evaluated prior to use in comparison to the previous Windows versions.

Objective

The objective of this module is to protect information processed in Windows 10, including on corresponding clients.

Not in Scope

Building on the requirements of module SYS.2.1 *General Client*, this module includes specific requirements that are to be taken into consideration and fulfilled in order to securely operate clients in the Windows 10 operating system. Therefore, the requirements included always have to be considered in connection with the requirements included in the SYS.2.1 *General Client* module. Protection against advanced and persistent threats must be implemented by complying with additional requirements of the different layers of the modernised IT-Grundschutz compendium.

Threat Landscape

For module SYS.2.2.3 *Windows 10 Clients*, the following specific threats and vulnerabilities are of particular importance:

Malware in Windows 10

Due to the high distribution of Windows operating systems and the backwards compatibility that often exists between system generations, the threat of malware and unauthorised penetration of the IT system is relatively high. Malware may have numerous functions and provide an attacker with extensive control options. Among other purposes, malware may be used to

obtain specific passwords, control systems remotely, disable protective software and collect data without authorisation. The most serious damage that can be caused by malware is the loss or corruption of information or applications. However, the reputational and financial damage that may result from malware may also be significant. Due to its widespread distribution, Windows is a primary target that is highly exposed to numerous attackers and types of malware attacks.

Software Vulnerabilities in Windows 10

Windows 10, including the numerous applications that come with it, is a very complex software product. If software errors in this product are detected too late, the crashes or errors that occur in using it may have far-reaching consequences (e.g. incorrect calculation results, incorrect decisions at the top management level and delays in business processes). Software vulnerabilities or errors may result in serious vulnerabilities in individual applications, the entire IT system or even in all the IT systems connected to it. Vulnerabilities in Windows may be exploited by attackers to inject malware, read data without authorisation or perform manipulations.

Integrated Cloud Functions

Windows 10 includes numerous features that are used to store and synchronise data using the services of Microsoft (“cloud services”). This results in the risk of these services being used (whether unwittingly or carelessly) for sensitive or personal data, as well. At the same time, storing data with third parties (which are usually abroad) can result in infringements of data protection law. If a user logs into a new device using an already activated Microsoft account, the Microsoft cloud services used by the user will be set up automatically on the device. The organisation's data may thus be synchronised accidentally to the private devices of the employees. As another example, one of Windows 10's default settings is to secure the BitLocker recovery key directly in the cloud using the Microsoft account, which amounts to providing critical cryptographic secrets to a third party.

Impairment of Software Features Due to Compatibility Issues

Software that ran successfully in previous versions of an operating system will not necessarily work with the current version of Windows 10. Possible reasons for this may include new security features or operating system properties, as well as the discontinuation of functions or services. As a result, use of the software may be limited or completely impossible. Examples of activated security features that may be the cause of potential compatibility issues with new versions of Windows include User Account Control (UAC), Kernel Patch Protection (when using 64-bit versions of the operating system) and the necessity of signed drivers that may no longer be available for older devices.

Incorrect Administration or Use of Windows 10

Windows 10 is a complex operating system whose security is mainly determined by its configuration. Due in particular to incorrect configurations of individual or multiple components, this impairs the security of the client itself and the infrastructure used. In general, each interface on an IT system not only provides the opportunity to use certain services of the IT system in an authorised manner, but also carries the risk of the IT system being accessed via these interfaces without authorisation. If, for example, user IDs and associated passwords can be obtained due to the incorrect configuration of Windows' own authentication mechanisms, the applications or IT systems protected may be used in an unauthorised manner.

Incorrect or improper use of devices, systems and applications may also jeopardise the security of Windows, especially if existing security safeguards are ignored, bypassed or switched off deliberately. Security incidents may occur when access rights are granted too generously, passwords are easy to guess, storage media containing backup copies are inadequately protected or workstations are not locked during temporary periods of absence. Another consequence of the incorrect operation of Windows systems or applications may include the accidental deletion or modification of data. Here, it is also possible that confidential information will be published – for example, if access rights are used improperly.

Requirements

The specific requirements of module *SYS.2.2.3 Windows 10 Clients* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User

Basic Requirements

For module *SYS.2.2.3 Windows 10 Clients*, the following requirements **MUST** be implemented as a matter of priority:

SYS.2.2.3.A1 Planning the Use of Cloud Services

Windows-10-based devices are closely interconnected with Microsoft’s cloud services. Prior to using Windows-10-based devices, a strategic decision **MUST** therefore be taken regarding which included cloud services are to be used or may be used, and to what extent.

SYS.2.2.3.A2 Selecting and Procuring a Suitable Windows 10 Version

The scope of functions and the provision of functional changes in a Windows 10 version **MUST** be selected while taking into consideration the determined protection needs, the purpose at hand and the feasibility of the required security safeguards. Based on the results of this review, the established procurement process **MUST** be complemented by the selection of the corresponding licence model and release path (CB, CBB or LTSB).

SYS.2.2.3.A3 Appropriate Patch and Change Management

In order to be able to document and evaluate all changes, all Windows 10 systems **MUST** be subject to patch and change management. For complex patches or changes, tests, control and cancellation points and distribution priorities **MUST** be defined within the framework of an implementation plan. After a functional update of the operating system, it **MUST** be checked whether all requirements from the IT-Grundschutz compendium and the internal specifications are still met.

SYS.2.2.3.A4 Telemetry and Data Protection Settings

The telemetry services (i.e. diagnostics and usage data that is transmitted to the U.S. by Microsoft and used to identify and resolve problems, improve services and products and personalise the system with unique identification features) cannot be switched off completely in the operating system. Therefore, appropriate safeguards **MUST** be implemented (e.g. at the network level) in order to ensure that this data is not transmitted to Microsoft.

SYS.2.2.3.A5 Protection Against Malware

Unless other mitigating safeguards of the same or a higher order have been implemented regarding the protection of the IT system against malware, the use of a specialised component for malware protection **MUST** be implemented on Windows 10 clients.

SYS.2.2.3.A6 Integration of Online Accounts into the Operating System [User]

Logging into the system and domain **MAY ONLY** be possible using the account of a self-operated directory service. The ability to log in using local accounts **SHOULD** be reserved for administrators. Online login accounts (e.g. Microsoft accounts or accounts from other providers of identity management systems) **MAY NOT** be used because doing so transmits personal data to the systems of the manufacturer.

Standard Requirements

For module SYS.2.2.3 *Windows 10 Clients*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

SYS.2.2.3.A7 Local Security Policies

All security-relevant settings **SHOULD** be configured, tested and checked regularly as needed. The security policies **SHOULD** be configured in accordance with the recommendations of the operating system manufacturer and the default behaviour unless the default behaviour contradicts other requirements pertaining to IT-Grundschutz or the organisation. Deviations **MUST** be documented and justified. All applications and components that are not needed **SHOULD** be disabled. Security policies **SHOULD** be set in any case, even if a given setting does not deviate from the default behaviour of a security policy that has not been set.

SYS.2.2.3.A8 Central Management of Client Security Policies

All settings of the Windows 10 client **SHOULD** be managed centrally and configured in accordance with the determined protection needs based on the internal policies. Technically infeasible configuration parameters **SHOULD** be documented, justified and coordinated with the security management.

SYS.2.2.3.A9 Secure Central Authentication of Windows Clients

Only Kerberos **SHOULD** be used for central authentication. A group policy **SHOULD** prevent the use of older protocols. If this is not possible, NTLMv2 **MUST** be implemented as an alternative. Authentication by means of LAN Manager and NTLMv1 **MAY NOT** be allowed within the organisation or production operating environments. The cryptographic mechanisms used **SHOULD** be configured and documented in accordance with the determined protection needs and based on the internal policies. Deviating settings **SHOULD** be justified and coordinated with the security management.

SYS.2.2.3.A10 Configuration for the Protection of Applications in Windows 10

The data execution prevention SHOULD be enabled for all programs and services (opt-out mode).

SYS.2.2.3.A11 Protection of Login Information in Windows 10

If the enterprise version of Windows 10 is installed directly (read: natively) on a hardware system, Virtual Secure Mode (VSM) SHOULD be enabled. In addition to activating VSM, Credential Guard SHOULD be enabled to thwart attacks on the authentication tokens and hashes stored in the system. If this is not possible, the local security authority (LSA) credential protection SHOULD be activated (Protected Process Light, PPL). Network logins from local accounts SHOULD be prohibited.

SYS.2.2.3.A12 File and Sharing Authorisations

Access to files and folders on the local system and to network shares SHOULD be configured in accordance with an authorisation and access concept. This specifically also includes the administrative shares that exist on the system by default. Users' write rights SHOULD be restricted to a defined area in the file system. In particular, users SHOULD not be granted write rights to folders of the operating system or of installed applications.

SYS.2.2.3.A13 Use of SmartScreen Features

The SmartScreen feature, which checks files and web content downloaded from the Internet and transmits personal data to Microsoft in the process under certain circumstances, SHOULD be disabled.

SYS.2.2.3.A14 Use of the Voice Assistant Cortana [User]

Cortana uses personal data such as voice data, user input, calendar and contact data, names of preferred locations and applications used, which is transmitted to Microsoft. For this reason, Cortana SHOULD be disabled.

SYS.2.2.3.A15 Use of Synchronisation Mechanisms in Windows 10

The synchronisation of user data with Microsoft cloud services and the process of sharing WLAN passwords SHOULD be disabled completely.

SYS.2.2.3.A16 Connection of Windows 10 to the Microsoft Store

The use of the Microsoft Store SHOULD be checked and evaluated with respect to compatibility with the data protection and security regulations of the organisation. The general installation of apps in Windows 10 is not bound to the connection to the Windows Store. As a consequence, this feature SHOULD be disabled unless it is required.

SYS.2.2.3.A17 Use of the Automatic Login Function

Storing passwords, certificates and other login information for automatic logins to websites and IT systems SHOULD NOT be allowed.

SYS.2.2.3.A18 Use of Windows Remote Support

The effects on the configuration of the local firewall SHOULD be taken into account when planning the Windows remote support procedures (this does not refer to RDP). Remote support SHOULD only be performed following an explicit invitation. When storing an invitation in a file, the file SHOULD be protected by a password. In every case, the user currently logged in SHOULD have to agree explicitly to starting a session. The maximum period of validity of the

invitation for remote support SHOULD have a reasonable length. If this service is not used, it SHOULD be disabled completely.

SYS.2.2.3.A19 Use of Remote Access via RDP [User]

The effects on the configuration of the local firewall SHOULD be taken into account when planning the remote access. The group of users authorised for remote desktop access (RDP) SHOULD be specified by assigning the corresponding user rights. In complex infrastructures, it SHOULD only be possible to reach the RDP target system via an intermediate RDP gateway. In order to use RDP, a check and its implementation SHOULD ensure that the following convenience functions are in accordance with the protection needs of the target system:

- the use of the cache
- the integration of printers
- the integration of removable media and network drives
- the use of file repositories and smartcard connections

If the use of remote desktop access is not planned, this SHOULD be disabled completely. The deployed cryptographic protocols and algorithms SHOULD comply with the internal specifications of the organisation.

SYS.2.2.3.A20 Use of User Account Control for Privileged Accounts

The configuration parameters of User Account Control (UAC) SHOULD represent a balance between user-friendliness and security for the privileged accounts. The decisions regarding the configuration parameters to be used SHOULD be documented. Furthermore, the documentation SHOULD include all accounts with administrator rights, and a regular check SHOULD be performed as to whether it is necessary to extend the rights.

Requirements in Case of Increased Protection Needs

Generic suggestions for module *SYS.2.2.3 Windows 10 Clients* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.2.2.3.A21 Use of the Encrypting File System (EFS) (CI)

Since the encrypting file system (EFS) protects the keys used by means of the password of the user account, a complex password SHOULD be used. In addition, restrictive access rights SHOULD protect the files encrypted using EFS. Instead of the administrator, a dedicated account SHOULD be the recovery agent. In this context, the private key of this account SHOULD be secured and removed from the system. In so doing, backups of all private keys SHOULD be created. When using EFS with local user accounts, the local password memories SHOULD be encrypted by means of syskey. This may not be applicable if the operating system feature Credential Guard is being used. When using EFS, the users SHOULD be trained regarding the proper handling of EFS.

SYS.2.2.3.A22 Windows PowerShell (CIA)

The execution of PowerShell and of WPS files SHOULD only be permitted for administrators. The execution of PowerShell SHOULD be logged centrally and the logs SHOULD be monitored. The execution of PowerShell scripts SHOULD be restricted using the command "Set-Execution Policy-AllSigned" in order to prevent any accidental execution of unsigned scripts.

SYS.2.2.3.A23 Advanced Protection of Login Information in Windows 10 (CI)

SecureBoot SHOULD be used on UEFI-based systems, and the status of the protected mode for the LSA credential store SHOULD be monitored during system startup (see also SYS.2.2.3.A11 *Protection of Login Information in Windows 10*). If remote maintenance of the client systems by means of RDP is intended, the "restrictedAdmin" option for RDP SHOULD be used for deployments in Windows 10 in a domain with the functional level 2012 R2 or higher.

SYS.2.2.3.A24 Activation of the Last Access Time Stamp (A)

In order to facilitate analysis after the system has been misused, the NTFS last access time stamp SHOULD be enabled. Prior to activation of the stamp, the effects of the activation on system performance SHOULD be checked. The results of the check and the decision regarding the activation SHOULD be documented.

SYS.2.2.3.A25 Handling Remote Access Features of Connected User Experience and Telemetry (CI)

In Windows 10, the Connected User Experience and Telemetry (CUET) component is an integral part of the operating system that, in addition to the telemetry feature, provides a remote access option for the local system to the operating system manufacturer. Remote access to the Windows 10 client by the operating system manufacturer SHOULD be logged by the network and blocked if required.

Additional Information

For more information about threats and security safeguards for module SYS.2.2.3 *Windows 10 Clients*, see the following publications, among others:

[TN408187]	Configuring Additional LSA Protection: Microsoft TechNet, March 2014, https://technet.microsoft.com/en-us/library/dn408187.aspx , last accessed on 05.10.2018
[TN621547]	Credential Guard - Overview: Microsoft, April 2017, https://docs.microsoft.com/de-de/windows/access-protection/credential-guard/credential-guard-requirements , last accessed on 06.09.2018
[TN986865]	Device Guard - Overview: Microsoft, https://technet.microsoft.com/de-de/library/dn986865.aspx , last accessed on 06.09.2018
[WIN10E]	Compare Windows 10 editions: Microsoft, https://www.microsoft.com/de-de/WindowsForBusiness/Compare , last accessed on 06.09.2018
[WINLSA]	Configuring Additional LSA Protection: https://docs.microsoft.com/de-de/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection , last accessed on 06.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.2.2.3 *Windows 10 Clients*:

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.1 5	G 0.1 6	G 0.1 7	G 0.1 8	G 0.1 9	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 5	G 0.2 6	G 0.2 8	G 0.2 9	G 0.3 0	G 0.3 1	G 0.3 2	G 0.3 6	G 0.3 9	G 0.4 5	G 0.4 6
SYS.2.2.3.A1	X			X	X							X				X		X	X
SYS.2.2.3.A2				X								X							
SYS.2.2.3.A3				X		X	X	X	X	X	X						X		
SYS.2.2.3.A4	X			X	X							X				X			X
SYS.2.2.3.A5						X	X	X			X						X		
SYS.2.2.3.A6	X				X											X			
SYS.2.2.3.A7				X				X		X	X		X	X					
SYS.2.2.3.A8				X				X					X	X	X				
SYS.2.2.3.A9				X				X					X	X					
SYS.2.2.3.A10				X		X	X			X	X						X		
SYS.2.2.3.A11				X							X								
SYS.2.2.3.A12				X	X		X						X		X				X
SYS.2.2.3.A13				X	X							X							X
SYS.2.2.3.A14	X			X	X							X							X
SYS.2.2.3.A15				X	X							X							X
SYS.2.2.3.A16				X	X						X	X							
SYS.2.2.3.A17		X	X	X				X					X						
SYS.2.2.3.A18	X			X				X					X	X					
SYS.2.2.3.A19	X			X	X			X					X	X					
SYS.2.2.3.A20				X	X						X		X	X	X				
SYS.2.2.3.A21		X	X	X	X														

SYS.2.2.3.A22				X			X											
SYS.2.2.3.A23				X	X		X											
SYS.2.2.3.A24				X								X						
SYS.2.2.3.A25	X			X				X				X			X			



SYS.2.3: Unix Clients

Description

Introduction

In addition to Windows, the operating system Linux (or more rarely, Unix) is being installed on an increasing number of clients. Examples of classic Unix systems include the BSD series (FreeBSD, OpenBSD and NetBSD), Solaris and AIX. Linux, meanwhile, is not a classic Unix system (the kernel is not based on the initial source code on which the development of the different Unix derivatives is based), but it is a functional Unix system. Since the configuration and operation of Linux and Unix clients are similar, all operating systems of the Unix family will be addressed in this module.

Linux is free software that is developed by the open-source community. In addition, there are providers that consolidate and maintain distributions comprising the Linux kernel and various software components while offering additional services. Derivatives of the distributions Debian, Red Hat Enterprise Linux or SUSE Linux Enterprise are frequently used. Furthermore, there are Linux distributions tailored to specific purposes and devices, such as Qubes OS, which attempts to achieve a high level of security with the help of virtualisation; IGEL Linux (a thin client); LibreElec for use on a home theatre PC (HTPC); or Kali Linux, a distribution specialised in security, computer forensics and penetration tests. Furthermore, clients may start live distributions without changing the present operating system.

While the market share of the Linux operating system on clients has increased in recent years, “classic” Unix systems in different derivatives continue to be used in specific operational environments. The quantity of previously selected software packages of a default installation of the common Linux distributions or the Unix derivatives increases the number of possible attacks; at the same time, however, Unix-like operating systems also offer comprehensive protection mechanisms. Typically, an IT system of this type is networked and operated as a client in a client-server network. Since clients are often operated in Unix or Linux for security reasons and it is not possible to rely on proper user behaviour (as is the case for all clients), the protection of Unix-like clients is of particular importance.

Objective

The objective of this module is to protect information created, processed, stored or sent on Unix clients. The requirements of the module mainly address Linux clients, but may be adapted generally for Unix clients. The present module largely does not differentiate between Unix and Linux; the term “Unix” refers to both Unix and Linux clients.

Not in Scope

This module includes basic requirements for operating Unix-like clients on commercially available IT systems. It specifies and adds specifics of Unix systems to the aspects addressed in module SYS.2.1 *General Client*. Although Apple's macOS is a Unix-like operating system, it is not addressed in this module; related recommendations can be found in module SYS.2.4 *macOS Clients*.

If the client is to be managed not by the organisation, but by a third party, the requirements of module OPS.3.1 *Outsourcing for Service Providers* must also be taken into consideration.

The present module only includes the Unix-like operating system that is usually involved in a basic installation of a Linux desktop distribution. In particular, the module does not include software that builds on such configurations, such as e-mail clients or Office software; the requirements in this regard can be found in layer APP.1 Client Applications of the IT-Grunds-chutz compendium. If the client has interfaces for data exchange (e.g. CD/DVD, USB, Bluetooth or WLAN), the security specifications of module SYS.3.4 *Mobile Storage Media* must be fulfilled.

Within the framework of this client module, it is assumed that, in addition to the administrator, only one unchanging person makes constant active use of an interactive user account. Clients used by several persons consecutively or simultaneously require additional safeguards not addressed within the framework of this module.

Threat Landscape

The following specific threats and vulnerabilities are of particular importance for module SYS.2.3 *Unix Clients*:

Malware

Malware is developed with the objective of executing unwanted and usually damaging functions. Malware is usually activated in secret without the knowledge or permission of the user. These days, malware provides an attacker with extensive communication and control capabilities, as well as a number of functions. Amongst other things, malware may be used to obtain specific passwords, control systems remotely, disable protective software and obtain data without authorisation. In particular, users who trust Unix-like systems to have a higher level of security right from the beginning are often more careless when handling unknown files.

Software from Third-Party Sources

When using Unix-like IT systems, it is not unusual to download and compile the software independently instead of installing ready-made software packages. If ready-made software packages are used, these often are not always installed from the existing package sources of the Unix derivative; they can also be procured from third-party sources without any further examination. Each of these alternative means of software installation entails additional risks because incorrect or incompatible software and malware may be installed.

Software Vulnerabilities or Errors

Numerous applications are usually available for installation on Unix-like IT systems. Since each of the applications to be installed may have software vulnerabilities and errors, the potential number of attacks increases unless it is ensured during the installation that only the required software is installed.

Exploitability of the Script Environment

Script languages are often used in Unix-like operating systems. Scripts are lists of individual commands that are stored in text files and opened in the command line (for example). Due to the large scope of functions of script environments, attackers may make extensive use of scripts for their purposes. Furthermore, it can be very difficult to contain enabled script languages.

Dynamic Loading of Jointly Used Libraries

The command line option “LD_PRELOAD” loads the stated library before any other libraries required in an application, and its functions are used by the application. An attacker could manipulate the operating system so that malicious functions are executed when using certain applications.

Incorrect Configuration

When using Unix-like operating systems, numerous applications requiring separate configurations are already installed within the framework of a default installation. Applications installed at a later point in time must also be configured separately, which means that numerous configuration files can be found on Unix-like operating systems.

Since these applications are configured independently of each other, the configuration options may be contradictory without this being visible from the individual settings. For example, one remote administration service may eavesdrop on a port blocked by packet filter rules, or Samba may inadvertently share its own home directory in the network. This way, the applications may accidentally provide additional functions or not provide important functions, which may make it more difficult to fulfil tasks using the client.

Requirements

The specific requirements of module *SYS.2.3 Unix Clients* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User

Basic Requirements

For module *SYS.2.3 Unix Clients*, the following requirements **MUST** be implemented as a matter of priority:

SYS.2.3.A1 Authentication of Administrators and Users [User]

In order to use the client, the users **MUST** be authenticated by the IT system. Administrators **MUST NOT** log in as root during normal operation. For system administration tasks, “sudo” or

an appropriate alternative with appropriate logging SHOULD be used. Multiple users SHOULD be prevented from logging into a device simultaneously.

SYS.2.3.A2 Selection of an Appropriate Distribution

An appropriate Unix derivative or Linux distribution MUST be selected based on the security requirements and the purpose. Support MUST be offered for the planned period of use of the operating system. All necessary application programs SHOULD be directly available without having to procure them from third-party sources.

Only application programs for which support is offered SHOULD be selected and installed. Operating system and application programs without regular security updates SHOULD not be used. Distributions with a rolling release model SHOULD not be used. Distributions in which the operating system is compiled independently SHOULD not be used in production environments.

SYS.2.3.A3 Cloud and Online Content [User]

Only absolutely necessary cloud and online services of the operating system MAY be used. The necessary cloud and online services SHOULD be documented. The settings of the operating system MUST be checked for conformity with the organisational data protection and security specifications and MUST be configured restrictively (or disabled).

SYS.2.3.A4 Installing Updates and Patches

The persons in charge MUST obtain information on vulnerabilities that have become known. Updates and patches MUST be installed as quickly as possible. A test system SHOULD first be used to check whether the security updates are compatible and do not cause any errors. When no patches are available for known vulnerabilities, other appropriate safeguards MUST be implemented in order to protect the client. The client MUST be rebooted promptly after the kernel has been updated. If this is not possible, live patching of the kernel MUST be enabled.

SYS.2.3.A5 Secure Installation of Software Packages

Only required applications MAY be installed. Applications that are no longer required MUST be uninstalled.

The integrity and authenticity of the software packages to be installed MUST always be checked. If the software to be installed is to be compiled from source code, this MAY ONLY be unpacked, configured and compiled using an unprivileged user account. Here, the software to be installed MUST NOT be installed in the root file system of the server in an uncontrolled manner.

If the software is compiled from the source text, the selected parameters SHOULD be documented appropriately. Based on this documentation, it SHOULD be possible to compile the source text in a transparent and reproducible manner at any time. All further installation steps SHOULD also be documented so that the configuration can be reproduced quickly in emergencies.

Standard Requirements

For module SYS.2.3 *Unix Clients*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.2.3.A6 Automatic Integration of Removable Drives [User]

Removable drives SHOULD not be integrated automatically. The integration of removable drives SHOULD be configured in such a way that all files are marked as non-executable (mount option “noexec”).

SYS.2.3.A7 Restrictive Granting of Access Rights for Files and Directories

User access to files and directories SHOULD always be restricted to the required minimum. In so doing, it SHOULD always be ensured that services and applications are only allowed to create, change or delete the files assigned to them. In directories in which all users have write privileges (e.g. /tmp), the sticky bit SHOULD be set.

SYS.2.3.A8 Use of Techniques to Restrict the Rights of Applications

In order to restrict the access rights of applications to files, devices and networks, AppArmor or SELinux SHOULD be used. The solutions with the best protection provided by the respective Unix derivative or Linux distribution SHOULD be selected. Instead of blacklisting, the necessary applications SHOULD be subject to whitelisting. Extensions regarding the restriction of rights SHOULD be used in enforcement mode or by means of appropriate alternatives.

SYS.2.3.A9 Passwords in the Command Line [User]

Passwords SHOULD NOT be transferred to programs as parameters.

SYS.2.3.A11 Prevention of Hard Disk Overload

Quotas for users or services SHOULD be set that leave enough capacity for the operating system. In general, different partitions SHOULD be used for the operating system and data. Alternatively, mechanisms of the file system used SHOULD also be used that only grant write rights to the root user once an appropriate level of capacity has been reached.

SYS.2.3.A12 Use of Appliances as Clients

It SHOULD be ensured that appliances are characterised by a level of security similar to that of clients on default IT systems. It SHOULD be documented how the corresponding security requirements are met when using an appliance. If it is not possible to unequivocally comply with the requirements, a declaration of conformity SHOULD be requested from the manufacturer.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.2.3 *Unix Clients* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.2.3.A13 Protection Against Unauthorised Logins (CIA)

Two-factor authentication SHOULD be used.

SYS.2.3.A14 Protection Against the Use of Unauthorised Peripheral Devices (CIA)

It SHOULD only be possible to use peripheral devices if they are included in a centrally managed whitelist. Kernel modules for peripheral devices SHOULD only be loaded and enabled if the devices can be found on the whitelist.

SYS.2.3.A15 Additional Protection Prior to Executing Undesired Files (CI)

Partitions and directories for which users have write rights SHOULD be mounted in such a way that no files can be executed (/noexec).

SYS.2.3.A16 Additional Protection of the Boot Process (CIA)

The boot loader and kernel SHOULD be signed by self-controlling key material, and unnecessary key material SHOULD be removed.

SYS.2.3.A17 Additional Prevention of Further Intrusion When Vulnerabilities Are Exploited (CI)

The use of system calls SHOULD be restricted to those that are absolutely necessary (e.g. by means of “seccomp”), particularly for exposed services and applications. The existing standard profiles and rules of SELinux and AppArmor, as well as alternative extensions, SHOULD be checked manually and adapted to one’s own security policy as required. If necessary, new rules and profiles SHOULD be drawn up.

SYS.2.3.A18 Additional Kernel Protection (CI)

Appropriate protective mechanisms which prevent the exploitation of vulnerabilities and further intrusion in the operating system (e.g. memory protection, file system protection and role-based access control) SHOULD be used with specially hardened kernels (for example, “grsecurity”, “PaX”).

SYS.2.3.A19 Hard Disk or File Encryption (CI)

Hard disks or the files stored on them SHOULD be encrypted. The related keys SHOULD NOT be stored on the IT system. “AEAD” SHOULD be used when encrypting hard disks and files. Alternatively, “dm-crypt” SHOULD be used in combination with “dm-verity”.

SYS.2.3.A20 Deactivation of Critical SysRq Features (CIA)

The SysRq functions that users may execute SHOULD be specified. In general, it SHOULD NOT be possible for users to trigger any critical SysRq functions.

Additional Information

For more information about threats and security safeguards for module *SYS.2.3 Unix Clients*, see the following publications, among others:

[ISiClient]	Whitepaper Absicherung eines PC-Clients (ISi-Client) [White Paper Securing a PC Client (ISi-Client): Federal Office for Information Security (BSI), 2011, https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Client/client_node.html , last accessed on 05.09.2018
[NISTSP800123]	Guide to General Server Security: NIST Special Publication 800-123, July 2008, https://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf , last accessed on 05.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module *SYS.2.3 Unix Clients*:

- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.28 Software Vulnerabilities or Errors
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.39 Malware
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.19	G 0.20	G 0.21	G 0.22	G 0.23	G 0.25	G 0.28	G 0.30	G 0.31	G 0.32	G 0.39	G 0.45	G 0.46
SYS.2.3.A1								X	X	X			
SYS.2.3.A2		X	X				X						
SYS.2.3.A3	X			X								X	X
SYS.2.3.A4		X	X			X	X				X		
SYS.2.3.A5		X	X				X				X		
SYS.2.3.A6			X	X	X	X						X	
SYS.2.3.A7	X		X	X				X	X	X			
SYS.2.3.A8	X		X	X				X	X	X			
SYS.2.3.A9			X	X	X			X	X	X		X	X
SYS.2.3.A11						X						X	X
SYS.2.3.A12	X	X	X	X	X	X	X	X	X	X	X	X	X
SYS.2.3.A13	X		X	X	X			X	X				
SYS.2.3.A14			X	X		X		X					
SYS.2.3.A15			X	X	X								
SYS.2.3.A16			X	X	X	X						X	
SYS.2.3.A17			X					X	X	X			
SYS.2.3.A18			X	X	X			X	X	X	X	X	X
SYS.2.3.A19	X			X	X								X
SYS.2.3.A20						X			X	X			



SYS.2.4: macOS Clients

Description

Introduction

macOS is a client operating system from Apple. It is based on Darwin, the free Unix operating system from Apple, which in turn is based on FreeBSD. macOS consists mainly of Darwin and the proprietary graphical user interface Aqua, as well as other applications and services. According to Apple's licence terms, macOS may only be installed on Apple's IT systems ("Macs"), which is why the particularities of these systems are also part of this module.

Objective

The objective of this module is to protect information which is processed on or transmitted by IT systems running macOS. Likewise, business processes and other IT systems must be protected from being impaired by IT systems running macOS. macOS clients must therefore be protected appropriately.

Not in Scope

This module focuses on protecting a Mac running macOS, which is operated as a stand-alone system or a client in a client/server network. This module therefore supplements the general aspects of module SYS.2.1 *General Client*, which also applies here. The possible use of macOS as a server operating system is not considered in this module. For professional settings, the Profile Manager tool and mobile device management service offer the option of remotely managing the Macs in use. These solutions offer extended configuration and administration functions which are not covered in this module. The relevant security aspects are covered in the module SYS.3.2.2 *Mobile Device Management (MDM)*. It should also be noted that the two Apple operating systems macOS (for Macs) and iOS (for iPhones and iPads) are closely interlinked. The module SYS.3.2.3 *iOS (for Enterprise)* should also be considered if iOS devices are used in addition to macOS.

Threat Landscape

For macOS, the following specific threats and vulnerabilities are of particular importance:

Uncontrolled Access to Outsourced Data

macOS offers a number of functions that are executed on centralised servers run by Apple. For example, Apple's iCloud can be used to store and synchronise data between different macOS and iOS devices. It is thus possible to start writing an e-mail on an iOS device and continue it on a Mac, for example. Since data (such as an e-mail draft) is temporarily stored on third-party

servers and is therefore no longer under the user's own control, unauthorised persons could, in principle, also access these servers and view and misuse the data stored or transmitted there.

Misuse of Apple IDs as Central Access Information for Apple Services

To use some macOS functions, a unique Apple ID is required as access information. The Apple ID provides central access to various Apple services such as iCloud, iMessage, iTunes and the App Store. If unauthorised persons attain Apple ID access information, they may be able to use these Apple services under a false identity and access information in iCloud.

Third-Party Functionality Integrated into the Operating System

macOS comes with interfaces to several third-party services, such as Google, Facebook and Twitter. These interfaces are often not required for business or even private use of a Mac, and they increase the potential points of attack.

Attacks on Wireless Interfaces

A Mac generally has Wi-Fi, Bluetooth and (depending on the model) additional wireless interfaces (e.g. infrared). With Wi-Fi functionality, for example, it is possible to exchange files directly between Apple devices (AirDrop). Furthermore, the Wi-Fi and Bluetooth functions can be used to synchronise macOS and iOS devices (Continuity). AirPlay makes it possible to send video and audio data to a compatible TV set. Attackers can attempt to misuse these wireless interfaces for attacks in order to intercept sensitive information between Macs, iPhones, iPads and other devices, or to compromise them in other ways.

Attacks on Applications with a Preview Function

Some of the applications integrated in macOS support a preview function for certain file formats (e.g. image files). These include the Finder, the Safari browser and the e-mail program integrated into macOS. For example, the preview function automatically displays the attachment of an e-mail if the file format is known. This means that excerpts of the e-mail attachment are displayed. An attacker could attempt to hide malicious code in the attachment of an e-mail. The preview function would display the e-mail attachment and possibly execute the malicious code, which in turn could compromise the Mac.

Insecure Protocols in macOS or macOS Applications

macOS and its applications use various protocols (e.g. AFP) for communication with central servers or other end devices. If these communication protocols do not have sufficient security mechanisms or are configured insecurely, the data transmitted could be read, falsified or otherwise misused without permission.

Requirements

The specific requirements of module *SYS.2.4 macOS Clients* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User

Basic Requirements

For module SYS.2.4 *macOS Clients*, the following requirements **MUST** be implemented as a matter of priority:

SYS.2.4.A1 Planning the secure use of macOS

The introduction of macOS **MUST** be planned carefully. In this regard, a concept for user management, administration and logging **MUST** be created. A decision **MUST** be made on where and how data will be stored. Plans **MUST** be made regarding how backups can be integrated into the organisation-wide backup concept. Plans **MUST** be made regarding how protection against malware can be integrated into the organisation-wide concept. The systematic installation of updates related to security and other aspects of macOS and applications **MUST** be planned. When switching the operating system to macOS, the applications required **MUST** be determined. If a Mac is operated on a data network, the network protocols to be used **MUST** also be taken into account.

SYS.2.4.A2 Using the security functions integrated into macOS

The integrated macOS protection mechanisms System Integrity Protection (SIP), Xprotect and Gatekeeper **MUST** be activated. Gatekeeper **MAY ONLY** allow signed programs to run as long as unsigned programs are not absolutely necessary.

SYS.2.4.A3 Administration of user accounts [User]

The administrator account created during the initial configuration of macOS **MAY ONLY** be used for administrative purposes. A standard user account **MUST** be created for normal Mac use. If a Mac is used by several users, a separate user account **MUST** be created for every user. The guest user account **MUST** be disabled.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module SYS.2.4 *macOS Clients*. They **SHOULD** be implemented as a matter of principle.

SYS.2.4.A4 Use of hard drive encryption

Hard drives **SHOULD** be encrypted, particularly for portable Macs (e.g. MacBooks). If the FileVault function integrated into macOS is used for this, the key material **MUST NOT** be stored online at Apple. The recovery key produced by FileVault **MUST** be stored in a secure place.

SYS.2.4.A5 Increasing the protection of data

The location services integrated into macOS **SHOULD** be deactivated. Downloaded data **SHOULD NOT** be opened automatically. Content from optical and other media **SHOULD NOT** be executed automatically.

SYS.2.4.A6 Using up-to-date hardware

When acquiring new Macs, current models SHOULD be purchased. If existing Macs are being used, a check SHOULD be performed to determine whether they are still receiving security updates from Apple. If the Macs are no longer supported by Apple, they SHOULD NOT be used.

SYS.2.4.A7 Two-factor authentication for Apple IDs [User]

Two-factor authentication SHOULD be activated for Apple ID accounts.

SYS.2.4.A8 No iCloud use for sensitive data [User]

Synchronisation of data between multiple devices via iCloud services such as Handoff SHOULD be prevented. Data SHOULD only be synchronised using self-operated services. Sensitive data SHOULD NOT be stored in iCloud. Drafts (e-mails, documents etc) SHOULD NOT be stored automatically in iCloud.

SYS.2.4.A9 Use of additional virus protection programs

If required, e.g. when operating a Mac in a heterogeneous network, virus protection solutions from third parties SHOULD be used in addition to the integrated protection mechanisms of macOS.

SYS.2.4.A10 Activating the personal firewall

The personal firewall integrated into macOS SHOULD be activated and configured.

SYS.2.4.A11 Device disposal

For any Mac disposal, the non-volatile memory (NVRAM) SHOULD be reset.

Requirement in Case of Increased Protection Needs

Generic suggestions for module SYS.2.4 *macOS Clients* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.2.4.A12 Activating the firmware password [User] (CI)

To prevent unauthorised booting of a Mac from another boot drive, secure firmware password queries SHOULD be activated in “command mode”. Considerations SHOULD be made as to whether a password should be queried via “full mode” during every startup.

Additional Information

For more information about threats and security safeguards for module “SYS.2.4 *macOS Clients*” see the following publications, among others:

[NIST800179]	NIST Special Publication 800-179: Guide to Securing Apple OS X 10.10 Systems for IT Professional
--------------	--------------------------------------------------------------------------------------------------

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.2.4 *macOS Clients*:

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.14	G 0.16	G 0.17	G 0.18	G 0.19	G 0.21	G 0.23	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.39	G 0.45	G 0.46
SYS.2.4.A1				X					X	X	X			X	X
SYS.2.4.A2	X				X	X	X						X		
SYS.2.4.A3				X			X			X	X	X			
SYS.2.4.A4	X	X	X		X					X					
SYS.2.4.A5	X				X	X	X	X							
SYS.2.4.A6				X				X							
SYS.2.4.A7	X			X	X										
SYS.2.4.A8	X			X	X				X					X	
SYS.2.4.A9	X				X	X	X						X		
SYS.2.4.A10				X	X		X					X	X		
SYS.2.4.A11	X			X	X				X					X	
SYS.2.4.A12	X	X	X		X	X	X			X	X				



SYS.3.1: Laptops

Description

Introduction

A laptop (or notebook) is a PC designed for mobile use. It has a compact design, peripheral devices such as a keyboard and monitor, batteries that make it temporarily independent from an external power supply and, in many cases, hardware components specially designed for mobile use. Laptops may be operated with all commonly used operating systems, such as Windows, Apple macOS or Linux. The devices are widely used in most organisations and, for some employees, they replace the traditional desktop PC.

Since laptops are frequently used as mobile devices, they are often not permanently connected to the organisation's LAN, but rather can choose between the Internet or other data networks (generally via a virtual private network, or VPN) in order to access the resources on the LAN. The infrastructure in a traditional office environment (which features controllable environmental factors, a stable power supply and restricted areas) cannot be assumed for the mobile use of laptops.

Objective

The objective of this module is to make the secure use of laptops possible in organisations and to make people aware of the specific threats to this type of device.

Not in Scope

In order to eliminate risks resulting from incorrect operation or accidental misuse of the laptop, it is necessary to select and install the operating system and software components carefully. The requirements to be met here depend on the operating system on the laptop, which is why they are set out in the client-specific modules – for example, *SYS.2.2.3 Windows 10 Clients*, *SYS 2.3 Unix Clients* or *SYS 2.4 macOS Clients*. In addition, requirements which apply to any type of client are not part of this module; they can be found in *SYS.2.1 General Client*.

How the respective data connection should be set up – for example, in WLAN configurations (see *NET.2.2 WLAN Usage*) or VPN connections (see *NET.3.3 VPN*) – is not covered here either.

In order to be able to detect attempted attacks and misuse, organisational requirements are especially necessary for laptops. The necessary requirements are considered in the course of implementing module *OPS.1.1.1 General IT Operation* and are therefore not considered here.

Threat Landscape

For module SYS.3.1 *Laptops*, the following specific threats and vulnerabilities are of particular importance:

Degradation Due to Changing Operating Conditions

Laptops are used in a very wide range of environments and are therefore subject to many threats. These threats include, for example, damaging environmental conditions such as excessively high or low temperatures, as well as dust and moisture. Mobile devices may also be damaged in transit. In addition, laptops communicate with unknown IT systems or networks (particularly while on the go), which always poses a potential risk. Here, for example, malware can be transmitted or sensitive information can be copied.

Theft

Employees regularly use their laptops outside the organisation. The devices are transported in cars or on public transportation, left in other peoples' offices during breaks or left unattended in hotel rooms. Due to these environmental factors, laptops are naturally exposed to a higher risk of theft. If a laptop is stolen, expenses are incurred in replacing the equipment and restoring it to working order. Sensitive data can also be disclosed to unauthorised persons as a result, which can lead to further damage. In many cases, this is significantly more severe than the mere material loss of the device.

Unregulated Changes of Laptop Users

If employees only need mobile IT systems in exceptional cases (e.g. for occasional business trips), it is often more practical to have multiple users share a small number of laptops. However, if a change of users involves simply handing a laptop over to the next employee, there is a risk that sensitive data may still be present on the device and that it may be infected with malware. After a while, it is also impossible to determine who used the laptop when, or who is currently using it. Unregulated changes of users that take place without memory scans and corresponding documentation may therefore restrict the availability of the device and result in residual data on the hard disk being read without authorisation.

Errors During Synchronisation

If data is edited locally on a laptop, it must be synchronised with the organisation's file servers whenever possible (e.g. when the employee logs in again via the VPN). However, this can corrupt the data. In general, settings must be specified prior to synchronisation to define how to handle any conflicts arising during data synchronisation – for example, whether the version on the laptop or the version also edited by another employee on the server should be updated without prompting when files have the same name, or whether the user should decide. This is frequently configured once and then forgotten. However, when data is then changed in a different order than was originally intended, important information may be quickly lost.

Data Loss During Mobile Use

For laptops, the risk of losing data is higher than for stationary systems. The reason for this may result from the theft or the loss of the device, but also from technical problems or a simple power outage. For example, the data on a laptop may be temporarily unavailable if the battery is empty. In some situations (involving older devices, for example), some data may be lost completely if the backup battery is also empty and the data has not been synchronised.

Data Theft Using Laptops

With laptops, data can very easily be exchanged with other IT systems (e.g. via WLAN, Bluetooth or GSM). Attackers can thereby retrieve or change information or take it with them unnoticed if open access to a laptop is possible. It is not always possible to analyse such incidents or secure evidence because the access attempts are often not logged accordingly. Attackers can also record all data transmitted over public WLANs that are not sufficiently secured and used by laptops to communicate, which can grant them access to the files on the organisation's network in the worst-case scenario.

Requirements

The specific requirements of module SYS.3.1 *Laptops* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Procurement Department, User, Head of IT

Basic Requirements

For module SYS.3.1 *Laptops*, the following requirements **MUST** be implemented as a matter of priority:

SYS.3.1.A1 Rules for Mobile Laptop Use

What employees should observe when taking laptops with them **MUST** be clearly regulated. In particular, which laptops may be taken outside the organisation, who may take them and what basic security measures should be followed **MUST** be specified. The users **MUST** be informed of the rules.

SYS.3.1.A2 Laptop Access Protection [User]

All laptops **MUST** have suitable access protection which prevents the device from being used without authorisation. Checks **MUST** be carried out to determine whether all employees are complying with the rules for correct handling of the access protection configured.

SYS.3.1.A3 Use of Personal Firewalls

A personal firewall **MUST** be active on laptops. The filter rules for the personal firewall **MUST** be configured as restrictively as possible. They **MUST** be tested regularly. The personal firewall **MUST** be configured in such a way that the users are not pestered by warnings they are not able to interpret.

SYS.3.1.A4 Use of Anti-Virus Programs [User]

Depending on the operating system installed and other available protective mechanisms, an anti-virus program **MUST** be installed and activated on all of the organisation's laptops. Care

MUST be taken to ensure that both the scan program and the signatures are always up to date. The users MUST be familiarised with the anti-virus software, and in particular with on-demand scans.

All of the data on the laptop MUST be checked regularly for malware. If the computer is infected, it MUST be examined in offline mode to determine whether the detected malware has already collected confidential data, deactivated any protective functions or downloaded any code from the Internet, for example.

The anti-virus software MUST search for malware if files are exchanged or transmitted. All encrypted files and Internet services (HTTP, FTP) used on the laptop MUST be sufficiently protected against malware.

In addition, care MUST be taken to ensure that users are not able to make any security-related changes to the settings of the anti-virus program.

SYS.3.1.A5 Data Backup [User]

All data which is saved locally on laptops MUST be backed up regularly. To this end, suitable backup methods MUST be selected depending on the volume of data. The backup process MUST be largely automated so that the users need to perform as few tasks as possible on their own.

Standard Requirements

For module SYS.3.1 *Laptops*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.3.1.A6 Security Policies for Laptops [Head of IT]

Security policies which govern how the devices may be used SHOULD be established for laptops. The users SHOULD be made aware of the protection needs for laptops and the data found on them. They SHOULD also be made aware of the specific threats to and the corresponding requirements for use. Furthermore, they SHOULD be informed of the types of information they may process on laptops.

SYS.3.1.A7 Orderly Issue and Return of Laptops [User]

If laptops are used by different people in turns, secure methods of handing laptops over to employees and returning them to the organisation SHOULD be defined. When a laptop changes users, any sensitive data present SHOULD be securely deleted. If the laptop is not reinstalled after the change of users, care SHOULD be taken to ensure that there is no malware on the system or any storage media connected to it. When they are issued a laptop, employees SHOULD also receive an information sheet on secure handling of the device.

SYS.3.1.A8 Secure Connection of Laptops to Data Networks [User]

Secure means of connecting laptops to internal or external networks and the Internet SHOULD be defined. Laptops SHOULD be effectively protected against malicious code, as well as against attacks from external networks and the Internet. To this end, the operating system and software installed on the laptops SHOULD always be kept up to date. Only authorised laptops SHOULD be able to connect to the organisation's internal network. Unnecessary interfaces SHOULD be deactivated on all laptops.

SYS.3.1.A9 Secure Remote Access from Outside the Office [User]

Data which is transmitted between a laptop outside the organisation and the organisation's internal network SHOULD be sufficiently secured using suitable measures – for example, using a VPN or TLS. The laptop itself SHOULD also be secured if data is exchanged with other IT systems.

SYS.3.1.A10 Synchronisation of Stored Data on Laptops [User]

The way in which data is transferred from laptops to the organisation's information domain SHOULD be regulated. If a synchronisation tool is used, care SHOULD be taken to ensure that synchronisation conflicts can be resolved, the synchronisation process is logged and the users are instructed to check the synchronisation logs.

SYS.3.1.A11 Safeguarding the Power Supply [User]

All users SHOULD receive information as to how they can best guarantee their laptop's power supply during mobile use. If spare batteries are available for the laptops, these SHOULD be stored and transported in appropriate cases.

SYS.3.1.A12 Reporting a Loss [User]

If a laptop is lost or stolen, this SHOULD be reported immediately. There SHOULD be clear reporting channels in every organisation for this purpose. If lost laptops reappear, there SHOULD be an investigation into whether they could have been manipulated. They SHOULD be completely reinstalled.

SYS.3.1.A13 Encryption of Laptops

The hard disks on a laptop SHOULD be encrypted. A secure algorithm SHOULD be used for encryption. The cryptographic keys SHOULD be generated randomly. The cryptographic keys SHOULD be documented appropriately.

SYS.3.1.A14 Suitable Storage of Laptops [User]

All users SHOULD be instructed in how laptops should be stored outside the organisation. While on the organisation's premises, laptops SHOULD also be secured against theft when they are not in use, or stored under lock and key.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.1 *Laptops* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.3.1.A15 Appropriate Selection of Laptops [Procurement Department] (A)

Before laptops are purchased, the persons in charge SHOULD carry out a requirements analysis. This SHOULD also include additional necessary hardware, such as docking stations and monitors. All possible devices SHOULD be assessed on the basis of the results. The purchase decision SHOULD be coordinated with the administrators and the technical personnel.

SYS.3.1.A16 Central Administration of Laptops (CI)

A suitable approach to the central administration of laptops SHOULD be defined, as this not only makes it easier to distribute software and information, but also makes it possible to better implement the organisation's own security policies. A tool for central laptop management SHOULD support all operating systems used to the greatest extent possible.

SYS.3.1.A17 Pooled Storage (A)

Unused laptops SHOULD be stored in an appropriately secured room. The room used for this purpose SHOULD meet the requirements of INF.5 *Technology Room*.

SYS.3.1.A18 Use of Anti-Theft Devices (CIA)

The anti-theft devices to be used for laptops SHOULD be regulated. In the context of mechanical devices, care SHOULD be taken to ensure that they have a good lock.

Additional Information

Currently there is no additional information on threats and security measures for module SYS.3.1 *Laptops*.

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.3.1 *Laptops*:

G 0.4 Pollution, Dust, Corrosion

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.39 Malware

G 0.45 Data Loss

Elementary Threats Requirements	G 0.4	G 0.14	G 0.16	G 0.17	G 0.19	G 0.22	G 0.39	G 0.45
SYS.3.1.A1	X	X	X	X	X	X	X	X
SYS.3.1.A2		X			X	X		
SYS.3.1.A3		X			X		X	
SYS.3.1.A4		X			X			
SYS.3.1.A5				X				X
SYS.3.1.A6	X	X	X	X	X	X	X	X
SYS.3.1.A7		X			X			
SYS.3.1.A8		X			X		X	
SYS.3.1.A9		X			X		X	
SYS.3.1.A10								X
SYS.3.1.A11								X
SYS.3.1.A12		X			X			
SYS.3.1.A13		X			X	X		
SYS.3.1.A14	X	X	X	X	X	X		
SYS.3.1.A15			X		X			
SYS.3.1.A16							X	
SYS.3.1.A17	X			X				
SYS.3.1.A18			X	X	X			



SYS.3.2.1: General Smartphones and Tablets

Description

Introduction

Smartphones are mobile phones that are equipped with a large, normally touch-sensitive display. Smartphones often combine a mobile phone, media player, personal information manager and digital camera in one device and provide the users with different applications and features, such as a web browser, an e-mail client or GPS. Furthermore, they are equipped with mobile phone, WLAN, and Bluetooth interfaces. In simple terms, tablets are smartphones with a large form factor that often are not capable of making phone calls using the mobile phone network. The term "phablets" describes hybrid devices that combine aspects of smartphones and tablets; they are not highlighted specifically in this module.

Objective

The objective of this module is to provide the persons in charge of security management and IT operations with information on the typical threats to smartphones and tablets. Furthermore, it seeks to provide the persons in charge with approaches to drawing up configuration profiles in accordance with protection needs. These configuration profiles may be distributed and managed using a central infrastructure for mobile device management (MDM). However, given the large number of different operating systems, it cannot be assumed as a matter of principle that the devices are integrated into an MDM system.

Not in Scope

This module does not deal with how specific operating systems of smartphones and tablets are secured; this is set out in detail in the modules for the respective systems, e.g. SYS.3.2.3 *iOS (for Enterprise)* or SYS.3.2.4 *Android*. Security requirements for operating an MDM system are described in SYS.3.2.2 *Mobile Device Management (MDM)*.

Threat Landscape

For module SYS.3.2.1 *General Smartphones and Tablets*, the following specific threats and vulnerabilities are of particular importance:

Loss of Mobile Devices

Since mobile devices are often small and constantly carried around, they can easily be forgotten, lost or stolen. In addition to the economic damage, the loss of confidentiality and integrity

of the data on the devices is particularly serious. An attacker may use a stolen mobile end device in order to access confidential information or IT resources of the organisation.

Lack of Operating System Updates

New versions of mobile operating systems and updates are released at regular intervals. For devices with manufacturer-specific extensions of the operating system, the manufacturers must first integrate the updates and versions into their versions before proceeding with distribution. These updates are usually provided for the latest device generation and for a number of older device generations. However, not all previous operating system versions are supplied with updates and security updates to the same extent; sometimes, operating systems are discontinued due to economic reasons. Vulnerabilities in the operating system of a discontinued device generation that have become known at a later point in time are then not provided with updates and remain open.

Software Vulnerabilities in Applications (Apps)

Apps may include vulnerabilities which can be exploited for local attacks or attacks via network connections. Furthermore, many apps are no longer maintained by third-party developers. As a consequence, security deficiencies identified cannot be remedied by appropriate updates.

Manipulation of Mobile End Devices

An attacker may gain access to the devices in order to manipulate files in a targeted manner. For example, they may change the configuration, start additional services or install malware. As a consequence, an attacker may tap communication links on the manipulated system (resulting in unwanted data leaks) or change rules as they require (e.g. to allow access from the Internet to the intranet).

Malware

Like any device connected to the Internet, mobile end devices are also threatened by malware. In comparison to PC operating systems, the risk of infection is currently lower, but cyber criminals are increasingly concentrating on these devices. If a device is infected, attackers can read, modify or delete data or gain access to the organisation's internal IT resources, for example.

Web-Based Attacks on Mobile Browsers

Browsers, along with many other apps, can display websites and web content. The devices may thus be affected by phishing attacks, drive-by exploits and other web-based forms of attack.

Misuse of Fitness or Location Data

The operating systems of many devices include specific features for managing fitness and location data. This often personal data is particularly sensitive and makes an attractive target for attacks, especially if it is collected and stored over a longer period of time (provided that these features have been enabled by the user).

As a consequence, the location of the employee can be identified by an attack on the device or the cloud ID of the employee. In addition to the consequences associated with data protection laws, this may lead to other attacks on the employee.

Misuse of Sensitive Data on the Lock Screen

Many mobile operating systems are equipped with a function that displays push messages and messages from activated widgets on the lock screen. This allows the user's confidential information to be disclosed to and exploited by unauthorised third parties. Voice assistants can also be used to access telephone functions and contact data even when a device is locked. This may also allow unauthorised third parties to access sensitive information.

Threats Caused by the Private Use of Mobile Devices

When employees are provided with company smartphones, tablets and phablets, they might also use the devices for private use without authorisation. This immediately results in several problems for the organisation's information security. For example, a user might install apps containing malicious functions without having requested any authorisation to do so or visit a website that infects the device with malware. Many apps installed privately by the user also are a risk to the organisational information stored on the device because they can send address books to unknown servers or gain direct access to e-mails or documents, for example. This can result in data leaks, or in data entering the organisation in an uncontrolled manner. Known examples of this involve social media and instant messaging apps.

Threats Related to Bring-Your-Own-Device (BYOD) Scenarios

If private end devices are used for work-related purposes, this results in a wide range of potential risks. For example, legal problems may arise in relation to the software licences. If, in an emergency, work-related data needs to be deleted from the device through the MDM system, this may also affect the user's private data.

In addition, those in charge of IT can no longer check every single device brought along by employees to check whether it can also be used for business purposes. As a consequence, inappropriate devices may be used and internal data protection and security requirements may thus be violated. Furthermore, the users are often personally responsible for having their devices serviced and repaired. During such repairs, company data could be viewed without authorisation (for example). The same threat exists if there is no regulation of what should be done with the data on the device if the employee leaves the organisation.

Requirements

The specific requirements of module SYS.3.2.1 *General Smartphones and Tablets* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User, Process Owner

Basic Requirements

For module SYS.3.2.1 *General Smartphones and Tablets*, the following requirements **MUST** be implemented as a matter of priority:

SYS.3.2.1.A1 Definition of a Strategy for Smartphones and Tablets

Prior to smartphones or tables being provided, operated or used by an organisation, the general strategy regarding the use and control of the devices **MUST** be defined. In so doing, it **MUST**, amongst other things, be specified who may access which information of the organisation.

SYS.3.2.1.A2 Definition of a Strategy for Cloud Usage

The organisation **MUST** define a general strategy for mobile end devices regarding cloud usage and information control, as well as protection of the information. Access to and usage of cloud services for information of the organisation **MUST** be clarified and specified. The users **MUST** receive regular training on the use of cloud services.

SYS.3.2.1.A3 Secure Basic Configuration for Mobile Devices

All mobile end devices **MUST** be configured such that the protection needs are adequately satisfied. To this end, an appropriate basic configuration of security mechanisms and settings **MUST** be established and documented. Functions that are not required **SHOULD** be disabled. The activation of communication interfaces **SHOULD** be regulated and reduced to the minimum required for official purposes. Unused interfaces **SHOULD** be disabled. If an organisation uses an MDM system, the MDM client **MUST** already have been installed when handing over the mobile end device.

SYS.3.2.1.A4 Use of an Access Control Mechanism [User]

Smartphones and tablets **MUST** be protected with an appropriately complex device lock code. Use of the screen locking feature **MUST** be required. The display of confidential information on the lock screen **MUST** be disabled. All mobile devices **MUST** automatically activate the screen lock after a reasonably short period of time. The duration **MUST** depend on the protection needs.

After several failed attempts to unlock the screen, the mobile device **SHOULD** perform a factory reset. The data or the encryption keys **SHOULD** be deleted securely in this process. Users **SHOULD** be prevented from selecting recently used passwords when changing a password. The number of passwords after which a password may be used again **SHOULD** be defined.

SYS.3.2.1.A5 Operating System and App Updates

A process **MUST** be established for operating system and app updates. The updates **MUST** be tested. In particular, previously required functions, security mechanisms and the enforcement of compliance requirements **SHOULD** be checked. Upon approval, the updates **MUST** be rolled out promptly. When selecting mobile devices to be procured, the organisation **MUST** already ensure that the manufacturer will provide security updates for the devices throughout the planned period of use. Older devices that are no longer provided with updates **MUST** be disposed of and replaced with devices supported by the manufacturer. In line with the security aspects at hand, apps **SHOULD** not be used either if they are no longer supported by the manufacturer.

SYS.3.2.1.A6 Data Protection Settings

App and operating system access to data and interfaces **MUST** be restricted appropriately. The data protection settings **MUST** be configured as restrictively as possible. In particular, access to cameras, microphones and geodata **MUST** be checked for conformity with the organisation's internal data protection and security specifications and **MUST** be restrictively configured (or disabled).

SYS.3.2.1.A7 Code of Conduct in the Event of Security Incidents [Process Owner, User]

In general, all security incidents **MUST** be reported and handled. If devices are lost or unauthorised changes to the device and the software are detected, the persons in charge **MUST** immediately initiate appropriate countermeasures.

The possible consequences of events critical to security **MUST** be examined. Ultimately, all necessary safeguards **MUST** be implemented in order to rule out any access to confidential and business-critical information of the organisation.

SYS.3.2.1.A8 No Installation of Apps from Insecure Sources

The installation of apps from alternative markets or the file system **MUST** be prevented.

Standard Requirements

For module SYS.3.2.1 *General Smartphones and Tablets*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

SYS.3.2.1.A9 Use of Functional Extensions

Functional extensions **SHOULD** only be used restrictively. If possible, functional extensions **SHOULD** not be used at all. The functional extensions **SHOULD** not have any automatic access to sensitive information. They **SHOULD** not be able to circumvent or change the specified basic configuration.

SYS.3.2.1.A10 Policy for Employees Regarding the Use of Mobile Devices [User]

There **SHOULD** be a binding policy for employees regarding the use of mobile devices. This policy **SHOULD** define how mobile devices are to be used and maintained. It **SHOULD** address the subjects of storage and loss reporting. Furthermore, uninstalling management software and rooting the device **SHOULD** be clearly prohibited.

SYS.3.2.1.A11 Storage Encryption

The non-volatile storage of the mobile device **SHOULD** be encrypted. Sensitive data on storage media that is also used (e.g. SD cards) **SHOULD** be encrypted.

SYS.3.2.1.A12 Use of Non-Personalised Device Names

The device name **SHOULD** not include any information regarding the organisation or the user.

SYS.3.2.1.A13 Rules Regarding Screen Sharing and Casting

A decision **SHOULD** be taken as to whether functions should be used to transmit screen content and audio or video content (screen sharing or casting). The functions **SHOULD** be regulated in organisational or technical terms. To this end, a corresponding agreement **SHOULD** be concluded with the users.

SYS.3.2.1.A14 Protection Against Phishing and Malware in Browsers

All mobile end devices SHOULD be protected against malware. In the browser used, “safe browsing” or the warning function for malicious content SHOULD be enabled.

SYS.3.2.1.A15 Disabling Download Boosters

Download boosters that route data via the servers of the manufacturer SHOULD be disabled.

SYS.3.2.1.A16 Disabling Unused Communication Interfaces [User]

Communication interfaces SHOULD only be activated when needed and in suitable environments. If an MDM system is used, the interfaces SHOULD be managed centrally via this system.

SYS.3.2.1.A17 Use of the SIM Card PIN

Any usage of the SIM card of the organisation SHOULD be protected by a PIN. The super PIN/PUK SHOULD only be used by the people in charge within the framework of the defined processes.

SYS.3.2.1.A18 Use of Biometric Authentication

If a biometric procedure is used for authentication (e.g. based on a fingerprint sensor), it SHOULD be checked whether similar or higher protection can be achieved compared to using a device password. If this is unclear or if the protection is worse, a biometric procedure SHOULD NOT be used. Users SHOULD be made aware that biometric features can be falsified.

SYS.3.2.1.A19 Use of a Voice Assistant

Voice assistants SHOULD only be used when this function is necessary. Otherwise, they SHOULD be disabled. In general, it SHOULD not be possible to use a voice assistant when the device is locked.

SYS.3.2.1.A20 Selection and Approval of Apps

Apps from public app stores SHOULD be reviewed and approved by the persons in charge. To this end, an approval process in which suitable assessment criteria are also defined SHOULD be developed. All approved apps SHOULD be published internally in a standard catalogue.

SYS.3.2.1.A21 Definition of Permissible Information and Applications on Mobile Devices [Process Owner, User]

The organisation SHOULD specify which information may be processed on the mobile end devices. The basis for the regulations SHOULD include both the classification of the organisation’s data and the conditions in which the data is processed on the devices.

End device users SHOULD only be allowed to install approved and checked apps from sources classified as secure.

SYS.3.2.1.A22 Integrating Devices into the Internal Infrastructure via VPN

Mobile end devices SHOULD only be integrated into the infrastructure of the organisation through a VPN. To this end, an appropriate method SHOULD be selected and used. Authentication SHOULD preferably be implemented and operated by means of certificates instead of using classic passwords.

SYS.3.2.1.A28 Using the Filter Option for Websites

If the institution already uses a reputation service or a corresponding proxy server, this SHOULD be stored as a global HTTP proxy for all installed browsers. If the proxy is only accessible in the internal network, the end devices SHOULD be integrated (either permanently or based on the apps used) using a VPN connection.

If the mobile devices are not integrated into the institution's existing proxy or reputation infrastructure, filtering options based on whitelists or blacklists or third-party content filters SHOULD be used for web browsers.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.2.1 *General Smartphones and Tablets* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.3.2.1.A23 Additional Authentication for Confidential Applications (CI)

All applications containing confidential data SHOULD be protected by an additional authentication mechanism.

SYS.3.2.1.A24 Use in a Closed User Group (CI)

The password for the access point (access point name, APN) of a closed user group SHOULD be complex. Authentication SHOULD use the CHAP protocol.

SYS.3.2.1.A25 Use of Separate Work Environments (CI)

If the employees are permitted to use business devices privately as well, solutions for isolated working environments SHOULD be used on the end devices. Where possible, only certified products (e.g. in line with the Common Criteria) SHOULD be procured for this purpose. The organisation's data SHOULD remain in the organisation's environment.

SYS.3.2.1.A26 Use of PIM Containers (CIA)

Information on the mobile devices SHOULD be encapsulated (e.g. in a PIM container). In addition, the data SHOULD be secured by separate authentication and data and transport encryption that is independent from the operating system.

SYS.3.2.1.A27 Use of Specially Secured End Devices (CIA)

Depending on the protection needs, organisations SHOULD use specially secured mobile devices that are certified for processing information in line with statutory information protection classifications.

SYS.3.2.1.A29 Use of an Organisation-Related APN (CA)

It SHOULD be checked whether an organisation-related access point to the mobile network (access point name, APN) can be used to limit the permitted device pool. The mobile service provider assigns all devices using this APN an IP address range that is coordinated with the organisation. For authentication, a complex password with a maximum of 64 characters SHOULD be agreed with the mobile service provider. When using an organisation-related APN, authentication SHOULD take place on the basis of the CHAP protocol.

SYS.3.2.1.A30 Restricted App Installation Using a Whitelist (CIA)

For higher protection needs, the users of the mobile end devices SHOULD only be able to install approved and tested apps. The MDM system SHOULD prevent other apps from being installed; alternatively, it SHOULD immediately remove apps that are installed without authorisation.

Additional Information

For more information about threats and security safeguards for module SYS.3.2.1 *General Smartphones and Tablets*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[BSICS052]	Mobile Device Management: BSI Publications on Cyber Security (BSI-CS 052), Version 1.0, March 2013, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_052.pdf , last accessed on 13.09.2018
[ISF]	The Standard of Good Practice for Information Security: Information Security Forum (ISF), June 2018
[NIST18001D]	Securing Electronic Health Record on Mobile Devices: NIST Special Publication 1800-1d, Draft, July 2015, https://nccoe.nist.gov/sites/default/files/nccoe/NIST_SP1800-1d_Draft_HIT_Mobile-StandardsControls.pdf , last accessed on 13.09.2018
[NIST800124]	Guidelines for Managing the Security of Mobile Devices in the Enterprise: NIST Special Publication 800-124, Revision 1, June 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf , last accessed on 13.09.2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 15.11.2017
[TR02102]	Cryptographic Mechanisms: Recommendations and Key Lengths: BSI TR-02102, Federal Office for Information Security (BSI), January 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , last accessed on 13.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.3.2.1 *General Smartphones and Tablets*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G0.14	G0.15	G0.16	G0.17	G0.18	G0.19	G0.20	G0.21	G0.22	G0.23	G0.24	G0.25	G0.26	G0.27	G0.28	G0.29	G0.30	G0.31	G0.32	G0.33	G0.34	G0.35	G0.36	G0.37	G0.38	G0.39	G0.40	G0.41	G0.42	G0.43	G0.44	G0.45	G0.46	
SYS.3.2.1.A1		X			X	X						X	X			X	X														X	X		
SYS.3.2.1.A2	X				X	X			X	X	X					X	X	X	X	X	X		X							X	X	X		
SYS.3.2.1.A3	X	X	X	X		X		X	X	X	X					X	X					X	X					X	X		X	X		
SYS.3.2.1.A4			X	X		X				X	X					X	X	X	X	X	X		X						X		X	X		
SYS.3.2.1.A5	X	X	X	X		X	X	X	X	X	X	X		X								X							X		X	X		
SYS.3.2.1.A6	X	X				X			X	X	X											X	X						X	X		X	X	
SYS.3.2.1.A7	X	X	X	X	X				X																					X	X	X		
SYS.3.2.1.A8																						X												
SYS.3.2.1.A9	X	X				X			X	X	X		X																	X	X			
SYS.3.2.1.A10			X													X																		
SYS.3.2.1.A11	X	X						X							X																		X	
SYS.3.2.1.A12	X																																X	
SYS.3.2.1.A13	X												X																				X	

SYS.3.2. 1.A14				X		X	X		X									X			
SYS.3.2. 1.A15	X				X			X													X
SYS.3.2. 1.A16		X			X				X									X	X		
SYS.3.2. 1.A17			X	X														X			
SYS.3.2. 1.A18			X	X	X	X			X									X		X	
SYS.3.2. 1.A19	X		X	X		X												X	X	X	X
SYS.3.2. 1.A20	X	X			X		X	X	X	X								X	X	X	X
SYS.3.2. 1.A21	X	X			X	X	X	X	X	X	X							X		X	X
SYS.3.2. 1.A22	X	X	X	X		X			X												X
SYS.3.2. 1.A23	X	X			X			X	X	X								X		X	X
SYS.3.2. 1.A24																					X
SYS.3.2. 1.A25	X	X	X	X		X		X	X	X								X		X	X
SYS.3.2. 1.A26	X	X	X	X		X			X	X	X							X		X	X
SYS.3.2. 1.A27	X	X	X	X		X		X	X	X								X	X		X
SYS.3.2. 1.A28																		X			
SYS.3.2. 1.A29																		X		X	

SYS.3.2. 1.A30		X		X		X	X			X	X			X		X			
-------------------	--	---	--	---	--	---	---	--	--	---	---	--	--	---	--	---	--	--	--



SYS.3.2.2: Mobile Device Management (MDM)

Description

Introduction

For many employees, smartphones, tablets and phablets have become an indispensable part of their work. However, the IT departments are having to provide ever greater numbers of such devices in many different designs while also ensuring adequate security. In addition, mobile end devices are exposed to particular risks and their administration differs in fundamental respects from other IT systems.

Consequently, a mobile device management (MDM) system is essential for regulated and secure operation of these devices, particularly in organisations with a large number of smartphones, tablets and phablets. With such software, the end devices can be managed centrally, security regulations can be implemented and emergency actions can be triggered. An MDM system thus ensures a consistent or at least comparable security standard on all devices.

Objective

This module shows how mobile end devices can be securely used by organisations with an MDM system and how the MDM system itself can be operated in a secure way.

Not in Scope

For the purposes of this module, mobile end devices are smartphones, tablets and phablets on which operating systems such as Android, iOS, Windows Phone and BlackBerry OS are installed. The security requirements for laptops and tablets with desktop operating systems are set out in other modules. The requirements of SYS.3.2.1 *General Smartphones and Tablets* must be considered. How the smartphones, tablets and phablets from different manufacturers are specifically secured is set out in detail in the modules for the respective operating systems, e.g. SYS.3.2.3 *iOS (for Enterprise)* or SYS.3.2.4 *Android*.

Threat Landscape

For module SYS.3.2.2 *Mobile Device Management (MDM)*, the following specific threats and vulnerabilities are of particular importance:

Insufficient Synchronisation with the MDM System

In order for the MDM system to be able to implement the regulations defined by the persons in charge on the mobile end devices, the devices must be regularly synchronised with the MDM system. If a device is not connected to the MDM system for a long period of time, new or updated regulations may not be installed, for example. In addition, if there is no connection to a lost device, the data can no longer be remotely deleted.

Improper MDM Administration

MDM solutions are complex applications that typically have several hundred different rules. Not all of the rules can be combined with one another, while others depend on one another. Due to administrative errors, the end devices may be exposed to a wide variety of threats which have a direct or indirect effect on the confidentiality, availability or integrity of the data and applications.

Inappropriate Rights Management in MDM Systems

The MDM system's rights management component decides who can perform which settings and who can access which data. If an employee is assigned the wrong role, there is the risk that they will be granted higher-level rights than they should have. For example, they could view data without authorisation or change settings on the device. It would also be possible for them to install and use apps (or cloud storage services, for example) which are not authorised in the organisation. This may result in leaks of the organisation's sensitive data or the violation of statutory data protection regulations.

Non-Existent or Weak Encryption of Communications Between the MDM System and End Devices

If the data connection between the mobile end device and the MDM server is not encrypted (or is encrypted using outdated algorithms) or insufficient key lengths are used, the confidentiality and integrity of all data transmitted will be at risk. For example, an attacker could consequently disguise their IT system as the MDM server and thus gain access to sensitive information, or even change settings on all of the organisation's mobile devices.

Unauthorised Creation of Movement Profiles Through the MDM System

With most MDM products, it is possible to determine where a device is located, and location-dependent data or apps can be released or blocked ("geofencing"). This results in detailed movement profiles for the devices, and thus also for the users. If this data is collected without the users being appropriately informed, the persons in charge may, under some circumstances, be in violation of data protection regulations. There is also a risk of attackers accessing this data. Geofencing can also be misused to unlawfully monitor employees.

Requirements

The specific requirements of module *SYS.3.2.2 Mobile Device Management (MDM)* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	

Basic Requirements

For module SYS.3.2.2 *Mobile Device Management (MDM)*, the following requirements **MUST** be implemented as a matter of priority:

SYS.3.2.2.A1 Determining a Strategy for Mobile Device Management

A strategy **MUST** be developed which determines how employees may use mobile end devices and how the devices are integrated into the organisation's IT structures. The protection needs of the information to be processed is a fundamental consideration in this regard. The strategy **MUST** cover at least the following aspects:

- Can the MDM system be operated as a cloud service?
- Should the MDM system be operated by the organisation itself?
- What support and response requirements does the MDM provider need to fulfil?
- What compliance requirements must be implemented?
- Which mobile devices and which operating systems must the MDM system support?
- Must the MDM solution be multi-client-capable? Does it guarantee the necessary separation of clients?
- Must cloud services be incorporated?
- Must document management systems be incorporated?
- Must the MDM system incorporate and manage peripheral devices, as well?
- Which operating model is to be used: private end devices (bring your own device, BYOD), personalised end devices (owned by the organisation) or non-personalised end devices (owned by the organisation and used jointly)?

The strategy **MUST** be specified in writing and approved by the CISO.

SYS.3.2.2.A2 Definition of Admissible Mobile End Devices

The mobile devices and operating systems that are authorised in the organisation **MUST** be determined. All authorised devices and operating systems **MUST** satisfy the requirements of the MDM strategy and fully comply with the organisation's security requirements. The MDM system **MUST** be configured such that only approved devices can access the organisation's information. If new mobile end devices are purchased, they **MUST** be on the list of admissible terminal devices.

SYS.3.2.2.A3 Selecting an MDM Product

When suitable MDM software is to be purchased, care **MUST** be taken to ensure that it satisfies all of the requirements specified in the MDM strategy. It **MUST** also be able to implement all technical and organisational security safeguards and support all admissible mobile devices.

SYS.3.2.2.A4 Distribution of the Basic Configuration to Mobile End Devices

All mobile end devices **MUST** be integrated into the MDM system as quickly as possible so that they can be configured and managed in accordance with the organisation's policies. When the devices receive the basic configuration, they **MUST** be set to factory settings. For devices which are already in use, all organisation-related data **MUST** be deleted first. An end device which has not been configured through the MDM system **MUST NOT** be able to access the organisation's information.

SYS.3.2.2.A5 Secure Basic Configuration for Mobile End Devices

All mobile devices **MUST** be configured such that the protection needs are adequately satisfied. To this end, an appropriate basic configuration **MUST** be established and documented. When mobile end devices are handed over to employees, the MDM client **MUST** already be installed. Otherwise, it **MUST** be possible for the users to install the client themselves.

SYS.3.2.2.A6 Logging and Device Status

The MDM system **MUST** log all security-relevant events and configuration changes. The data collected **MAY NOT** be viewed by unauthorised persons and **MUST** be saved in an unalterable fashion. Legal and internal regulations **MUST** also be met with regard to logging. The logs generated by the MDM system **MUST** be checked regularly for unusual entries. The lifecycle of a mobile device (including its configuration history) **SHOULD** be sufficiently logged and centrally retrievable. If required, the administrator **SHOULD** be able to determine the current status of the managed devices (device audit).

SYS.3.2.2.A20 Regular Review of the MDM System

Security settings **MUST** be checked regularly. For new operating system versions of the mobile devices, it **MUST** be checked in advance whether the MDM system fully supports them and whether the configuration profiles and security settings are still effective and sufficient. Deviations **MUST** be corrected. The access rights assigned to users and administrators **MUST** be checked regularly to ensure that they are still appropriate (minimum principle)

Standard Requirements

For module SYS.3.2.2 *Mobile Device Management (MDM)*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

SYS.3.2.2.A7 Selection and Approval of Apps

Apps from public app stores **SHOULD** be reviewed and approved by the persons in charge. To this end, an approval process in which suitable assessment criteria are also defined **SHOULD** be developed. All approved apps **SHOULD** be published internally in a standard catalogue and should be available there for the users. Apps **SHOULD** be installed, uninstalled and updated via the MDM system in line with the requirements of the planned deployment scenario. The MDM system **SHOULD** force the installation, uninstallation and update process as soon as a connection to the mobile device is established.

SYS.3.2.2.A8 Determining Admissible Information on Mobile End Devices

The organisation SHOULD specify which information may be processed on the mobile devices under which conditions. The basis for the regulations SHOULD be the classification and protection needs of the information and the conditions in which the data is processed on the devices (e.g. in sealed containers). The persons in charge SHOULD configure the MDM system on the basis of these regulations so that it can implement them on all mobile devices. The users SHOULD be informed of the regulations in an appropriate manner.

SYS.3.2.2.A9 Selecting Security Apps

In order to enforce the necessary level of security, appropriate security apps SHOULD be selected for the end device. The security apps SHOULD be automatically installed by the MDM system.

SYS.3.2.2.A10 Secure Connection of Mobile End Devices to the Organisation

The connection between the mobile devices and the MDM system SHOULD be appropriately secured. The connection of the mobile end devices to the organisation's network SHOULD be appropriately secured. If data is transmitted between the mobile devices and the organisation's IT network, appropriate safeguards (e.g. VPN) SHOULD be implemented to prevent unauthorised persons viewing and modifying the data.

SYS.3.2.2.A11 Authorisation Management in MDM Systems

An authorisation concept, or access control policy, SHOULD be created, documented, and applied to the MDM system. The user groups and administrators SHOULD only be granted as many authorisations for the MDM system as are necessary for the fulfilment of their tasks (minimum principle). Whether the rights assigned are still appropriate and relevant for their tasks SHOULD be reviewed at regular intervals.

SYS.3.2.2.A12 Secure MDM Operating Environment

The MDM system itself SHOULD be secured using technical safeguards in order to satisfy the protection needs of the information which is stored or handled. The underlying operating system SHOULD be hardened and all necessary patches SHOULD be applied. Access authorisations and routes SHOULD be configured according to the organisation's security concept.

SYS.3.2.2.A21 Administration of Certificates

Certificates for the use of services on the mobile device SHOULD be installed, uninstalled and updated centrally via the MDM system. The installation of untrusted and unverifiable (root) certificates by the user SHOULD be prevented by the MDM system. The MDM system SHOULD support mechanisms to verify the validity of certificates.

SYS.3.2.2.A22 Remote Deletion and Decommissioning of End Devices

The MDM system SHOULD ensure that all data on the mobile device can be deleted remotely (remote wipes for existing data connections). If external storage devices are used in the mobile device, the system SHOULD check whether these should also be deleted in a remote wipe. This function SHOULD be supported by the MDM system.

The process for decommissioning the mobile device (unenrollment) SHOULD ensure that no sensitive data remains on the mobile device or integrated storage media. This applies in particular if the unenrollment is to be carried out remotely.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.2.2 *Mobile Device Management (MDM)* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.3.2.2.A14 Use of External Reputation Services for Apps (CI)

If the administrators of an organisation are not able to select the admissible apps and users are able to install apps on their devices themselves, a reputation service SHOULD be used. This is an external service that evaluates apps according to specified criteria and provides the results to the customer. The MDM system SHOULD then use this information to at least limit the installation of apps.

SYS.3.2.2.A17 Monitoring the Use of Mobile End Devices (I)

MDM solutions allow for monitoring of how mobile end devices are used. Appropriate criteria SHOULD be defined and used as a basis for monitoring devices without violating legal or internal provisions.

SYS.3.2.2.A19 Geofencing (CI)

Using geofencing policies, it is possible to allow or prohibit specific functions or apps only in pre-defined locations. A geofencing policy SHOULD ensure that devices with sensitive information cannot be used outside a pre-defined geographical area. Leaving the geographic area SHOULD result in the selective deletion of classified information or the complete deletion of the device. Before the device is selectively or completely deleted, the administrators in charge, the security management and the user SHOULD be informed. The deletion SHOULD take place only with a reasonable time delay. Areas in which these additional security measures are required SHOULD be identified based on analysis of the protection needs. They SHOULD then be implemented in compliance with the legal and internal provisions.

SYS.3.2.2.A23 Enforcing Compliance Requirements (CI)

A solution from the MDM provider SHOULD be used to detect violations of the organisation's regulations or even manipulation of the operating system. The following actions SHOULD be taken if violations of regulations or manipulations of the operating system are suspected. To this end, corresponding functions should be made available:

1. autonomous issue of warnings
2. autonomous locking of devices
3. deletion of the organisation's confidential information
4. deletion of the entire device
5. prevention of access to company apps
6. prevention of access to the organisation's systems and information

If a violation or manipulation is suspected, an alarm SHOULD be sent to the administrators in charged and the security management in the organisation.

Additional Information

For more information about threats and security safeguards for module SYS.3.2.2 *Mobile Device Management (MDM)*, see the following publications, among others:

[BSICS052]	Mobile Device Management: BSI Publications on Cyber Security (BSI-CS 052), Version 1.0, March 2013, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_052.pdf , last accessed on 13.09.2018
[BYOD]	White Paper on Consumerisation and BYOD: Federal Office for Information Security (BSI), Version 1.2, July 2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_BYOD_pdf.pdf , last accessed on 07.09.2018
[NIST18001D]	Securing Electronic Health Record on Mobile Devices: NIST Special Publication 1800-1d, Draft, July 2015, https://nccoe.nist.gov/sites/default/files/nccoe/NIST_SP1800-1d_Draft_HIT_Mobile-StandardsControls.pdf , last accessed on 13.09.2018
[NIST800124]	Guidelines for Managing the Security of Mobile Devices in the Enterprise: NIST Special Publication 800-124, Revision 1, June 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf , last accessed on 13.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.3.2.2 *Mobile Device Management (MDM)*:

- G 0.11 Failure or Disruption of Service Providers
- G 0.13 Interception of Compromising Interference Signals
- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.17 Loss of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.45 Data Loss

Elementary Threats	G 0.11	G 0.13	G 0.14	G 0.15	G 0.16	G 0.17	G 0.18	G 0.19	G 0.21	G 0.22	G 0.23	G 0.24	G 0.25	G 0.28	G 0.29	G 0.30	G 0.31	G 0.32	G 0.36	G 0.37	G 0.38	G 0.39	G 0.45
SYS.3.2.2.A1							X								X								
SYS.3.2.2.A2							X																
SYS.3.2.2.A3	X						X																X
SYS.3.2.2.A4		X	X						X	X	X					X	X		X			X	
SYS.3.2.2.A5		X	X						X	X	X					X	X		X			X	
SYS.3.2.2.A6																X	X	X		X			
SYS.3.2.2.A7			X		X			X	X	X	X	X	X		X	X	X	X	X			X	
SYS.3.2.2.A8			X			X																	
SYS.3.2.2.A9			X		X	X		X	X	X	X			X		X			X		X		X
SYS.3.2.2.A10				X	X					X													
SYS.3.2.2.A11																X					X		
SYS.3.2.2.A12											X					X		X			X		
SYS.3.2.2.A14			X		X			X		X	X			X		X			X			X	
SYS.3.2.2.A17															X	X	X	X		X			

SYS.3.2.2. A19		X																			
SYS.3.2.2. A20					X	X	X		X				X	X	X	X					
SYS.3.2.2. A21		X	X		X	X		X	X				X	X	X	X	X		X		
SYS.3.2.2. A22		X	X	X	X	X	X			X			X	X			X		X		
SYS.3.2.2. A23				X				X	X				X								



SYS.3.2.3: iOS (for Enterprise)

Description

Introduction

Mobile devices are permanent companions in today's information society. They are always on-line, which means that they are connected to the Internet or the organisation's internal network, and thus offer access to digital information at all times. Communication takes place via various interfaces, such as GSM/UMTS/LTE, WLAN, and Bluetooth.

Due to their modern and simple control concepts and high performance, smartphones and tablets are very common nowadays. This also includes the mobile devices produced by Apple, i.e. iPhone and iPad, which run on the iOS operating system. Originally, these devices were designed for private use. Due to the reshaping of infrastructures and the ways in which information is collected and processed, however, they are also being used more and more frequently in a professional environment, where they are even replacing laptops in some cases.

Through the integration of business functions, iOS has (as of version 4) been gradually extended for use in companies and public authorities and functions have been integrated for management from an organisation's point of view. This includes, among other things, Apple's program to enrol devices in a centralised manner, as well as options such as single sign-on (SSO).

Objective

The objective of this module is to show how devices operated with iOS (for Enterprise) can be used securely in organisations. Requirements are presented for the settings of the iOS-based end devices, which can be distributed to the end devices in the form of configuration profiles. iOS configuration profiles include uniformly defined settings (e.g. for security policies or individual system aspects) for managing iOS-based devices in a uniform and centralised manner and configuring them automatically.

Not in Scope

This module includes basic requirements which must be observed and fulfilled when operating iOS-based devices which are integrated into the organisation's processes. Requirements for the integration into the organisation's security or collaboration infrastructure are not the focus of this module. Through mobile device management (MDM), it is possible to manage devices centrally and roll out configuration profiles for specific user groups or intended purposes. Using an MDM system, safeguards can also be implemented in a uniform way. This module assumes that the iOS devices to be managed are integrated into an MDM infrastructure. Situations in which a small number of devices (i.e. fewer than 10) are to be managed without an MDM system due to the economic aspects at hand can be considered justifiable exceptions. Requirements for the operation of MDM systems can be found in module SYS.3.2.2 *Mobile Device*

Management (MDM). For smaller environments, the Apple Configurator can also be used to roll out the requirements listed in this module to several end devices. General and comprehensive aspects of the operation of smartphones and tablets (regardless of the respective operating systems) can be found in module SYS.3.2.1 *General Smartphones and Tablets*.

Threat Landscape

For module SYS.3.2.3 *iOS (for Enterprise)*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Poor Access Protection

iOS-based devices are protected against unauthorised access by passcodes. If this function is not activated or an easy-to-guess code is used (and can thus be bypassed), there is a higher risk of unauthorised parties accessing iOS-based devices. Moreover, the device code used is an essential element of the entropy of certain encryption codes.

Jailbreaking

In most previous versions of the iOS operating system, vulnerabilities were found which made it possible to circumvent the security framework established by Apple and thereby access system processes and protected memory areas. “Jailbreaks” exploit these vulnerabilities as a means of using alternative app stores or extensions undesired by Apple (for example). Jailbreaking techniques are used by attackers in order to install malware or perform other harmful manipulations on the iOS-based device.

Concentration of Risk When One User Account (Apple ID) Is Used for All Apple Services

With the Apple ID, it is possible to centrally access all services made available by Apple (e.g. iMessage, FaceTime, iCloud, App Store, iTunes, iBook Store, iPhone Search or Synchronisation Services). If unauthorised persons obtain access to an inadequately secured Apple ID, they might, under certain circumstances, use these Apple services under a false identity, disrupt the availability of the Apple ID-based services, remotely localise iOS-based devices, reset all data or access information from the iCloud service. Especially in the case of activated iCloud backups, an attacker may be able to clone the data stored on a user's iOS device.

Missing Operating System Updates on Old Devices

New versions and updates of the iOS operating system are released at regular intervals. They are usually provided for the latest device generation and for a number of older device generations (see additional information). However, not all previous operating system versions are supplied with updates and security updates to the same extent. Vulnerabilities which have since become known in the operating system of a discontinued device generation will no longer be closed by updates.

Software Vulnerabilities in Apps

Apps for iOS can include vulnerabilities which can be exploited for local attacks or attacks via network connections. Furthermore, many apps are no longer maintained by third-party developers. There is the risk that identified security deficiencies will not be remedied by corresponding updates.

Deeper Integration for Pre-Installed Apps and Their Functions

In its operating system, Apple delivers deeply integrated and pre-installed apps (e.g. the Mail and Clock apps) as well as interfaces to services of third-party providers (such as Twitter or Facebook). These apps are partially designed with higher authorisations than apps that can be downloaded from the App Store, which increases the number of possible attacks on the iOS-based device. Using non-deletable or non-configurable interfaces is not desired in most cases when the device is used for official business purposes, and it also increases the number of possible attacks on the device.

Misuse of Biometric Authentication

The iOS operating system contains special functions that can be simplified by biometric authentication procedures such as the Touch ID fingerprint sensor or Face ID face recognition. These functions include, for example, activating the device in a simplified manner or shopping in iTunes and the App Store. Biometric security functions can be bypassed with sufficient effort – for example, by reconstructing an artificial finger on the basis of a digitally cleaned fingerprint. Up to 48 hours after the last unlock, which is the maximum time window for misuse, the device will accept activation via biometric procedures.

Misuse of Fitness, Health or Location Data in iOS

The iOS operating system includes special functions for managing fitness, health and location data. This data is particularly sensitive and an attractive target for attacks, especially if it is collected and stored over a longer period of time.

Misuse of Sensitive Data on Locked Devices

The iOS operating system is equipped with a function that displays push messages and messages from activated widgets on the lock screen. Without lock screen protection, there is the risk that sensitive information of the user will be disclosed to unauthorised third parties and thereby exploited. Using the language assistant Siri, it is possible to access telephone functions and contact details even when the device is locked. This may also enable unauthorised third parties to access sensitive information.

Misuse of Data Stored on iOS-Based Devices

Due to the many functions and extension options, an iOS-based device often contains sensitive data, such as e-mails, documents, text messages, passwords, credit card details or health-related data. There is the risk that this data will be misused if perpetrators get hold of the device after it is lost, stolen or disposed of, or if they obtain access to the data by technical means.

Improper Access to Outsourced Data

For a number of iOS-specific functions, the infrastructure operated by Apple must be used. When using the iCloud Keychain, iMessage, FaceTime, Siri, Continuity, Spotlight Suggestions functions, or iCloud for creating encrypted backups or working jointly on documents, the data between different devices or users is always synchronised via the Apple infrastructure. Push messages for iOS-based devices are also transmitted via this infrastructure. Therefore, there is a general risk that unauthorised persons will access Apple servers and misuse the data stored or transmitted there for their own purposes.

Web-Based Attacks on Browsers

Browsers, along with many other iOS-based apps, can display websites and web content. iOS-based devices may thus be affected by phishing attacks, drive-by exploits and other web-based forms of attack.

Insufficient Specifications for Licence Management

Managing software licences is one of the core tasks of IT compliance. An organisation must therefore define clear responsibilities and regulations. However, the subject of app licences is often not dealt with adequately. As part of general compliance, the persons in charge at the organisation must ensure that their employees do not commit licence violations.

Requirements

The specific requirements of module SYS.3.2.3 *iOS (for Enterprise)* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	

Basic Requirements

For module SYS.3.2.3 *iOS (for Enterprise)*, the following requirements **MUST** be implemented as a matter of priority:

SYS.3.2.3.A1 Strategy for Using iOS Devices

If an MDM system is used, the devices **MUST** be managed and configured via this system. There **MUST** be a strategy for using iOS devices that defines aspects such as the selection of end devices or backup strategies. Moreover, it **MUST** be regulated whether additional apps of third-party providers are to be used.

SYS.3.2.3.A2 Planning the Use of Cloud Services

Prior to using iOS-based devices, the extent to which cloud services should or may be used **MUST** be defined strategically. Consideration **SHOULD** be given to the fact that iOS-based devices are closely linked with Apple's iCloud services as a matter of principle, right from the point they are activated with an Apple ID. It **SHOULD** therefore be checked whether the Apple Device Enrollment Program (DEP) can be used, which makes it possible to do without Apple IDs.

SYS.3.2.3.A7 Preventing Unauthorised Deletion of Configuration Profiles

In order to ensure that configuration profiles cannot be deleted without authorisation, suitable technical or organisational regulations **MUST** be established and implemented. Users of mobile devices **SHOULD** be made aware of the intention and purpose of the security measures.

Standard Requirements

For module SYS.3.2.3 *iOS (for Enterprise)*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.3.2.3.A10 Use of Biometric Authentication

For iOS-based devices with biometric authentication features such as Touch ID or Face ID, these features SHOULD be approved for users as an alternative to unlocking the device if the need for users to use more complex device codes is addressed in both organisational and technical terms at the same time. If Touch ID or Face ID is activated, users SHOULD be made aware of the fact that biometric features can be falsified.

SYS.3.2.3.A11 Use of Non-Personalised Device Names

To prevent the user and the device code from being guessed in certain circumstances, the device name SHOULD not contain any personal names or organisational features.

SYS.3.2.3.A12 Using Organisation-Related Apple IDs

Instead of the user's personal Apple ID, the iOS-based device should be used with an organisation-related Apple ID. As an additional precaution to prevent means of payment (credit cards) for official business purposes from being misused, Apple's Volume Purchase Program (VPP) SHOULD be used.

SYS.3.2.3.A13 Using the Configuration Option "Restrictions under iOS"

All iOS functions or services that are not needed or allowed SHOULD be disabled. Based on the intended purpose and the underlying need for protection, the following aspects in particular SHOULD be checked: lock screen, unified communication, Siri, background image, connection to host systems and diagnostic and usage data.

SYS.3.2.3.A14 Using the iCloud Infrastructure

Before the extensive or selective usage of the iCloud infrastructure is approved, the compatibility of Apple's general terms and conditions with the internal policies with regard to availability, confidentiality, integrity and data protection SHOULD be assessed. If use of the iCloud infrastructure is allowed, the authentication with the iCloud web service SHOULD take place by means of two-factor authentication. Using managed apps, iCloud use for purely business purposes SHOULD also be reduced to a minimum or completely excluded.

SYS.3.2.3.A15 Using the Continuity Functions

If using the iCloud infrastructure has not been generally prohibited by the organisation's security management department, the compatibility of the Continuity functions (AirDrop and Handoff) with the internal policies SHOULD be assessed while taking the aspects of confidentiality and integrity into account. Based on the assessment results, the extent to which these functions are technically and organisationally restricted SHOULD be regulated.

SYS.3.2.3.A17 Using the Device Code History

In order to maintain the confidentiality of the device code used and to prevent rapid repetitions of passwords utilised by the user, the number of unique codes required before the first repetition is allowed SHOULD be defined with an appropriate value in the configuration profile.

SYS.3.2.3.A18 Using the Configuration Option for the Safari Browser

The browser policies already established in the organisation SHOULD also be implemented accordingly for Safari by means of technical and organisational safeguards. The already established requirements for browsers on stationary and portable PCs SHOULD be used as a basis for protecting the iOS-based devices, and the application scenarios and operational environment of the devices SHOULD be taken into consideration.

SYS.3.2.3.A20 Integrating Devices into the Internal Infrastructure via VPN

iOS-based devices SHOULD be integrated into the infrastructure via a VPN. Depending on the protection needs, purpose and technical possibilities of the VPN server, a VPN connection SHOULD be realised on the basis of IKEv2, IPSec, L2TP, PPTP or SSL/TLS technologies. Authentication SHOULD preferably be implemented and operated by means of one-time passwords and certificates instead of using classic passwords.

SYS.3.2.3.A21 Approval of Apps and Integration of the Apple App Store

If additional apps from third-party providers are used (see SYS.3.2.3.A1), the internal software approval process or the validation and approval of applications (apps) from the Apple App Store MUST be supplemented by the persons in charge. In order to support the organisation's internal app approval processes, the MDM system used SHOULD allow filtering on the basis of whitelists, blacklists or app reputation services.

All approved applications SHOULD be published internally in a standard catalogue and made available to the users. As an aid to ensure that the apps required are adequately available to the authorised users when needed, Apple's Volume Purchase Program (VPP) for companies can be integrated into the MDM infrastructure. Another aspect of using the VPP is that the Apple IDs used do not have to be stored with a means of payment. Payments for apps in the App Store SHOULD NOT be confirmed using biometric methods.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.2.3 *iOS (for Enterprise)* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.3.2.3.A23 Using Automatic Deletion of Configuration Profiles (CI)

Using automatic deletion of configuration profiles, it SHOULD be ensured that devices which cannot be constantly accessed online will lose their existing access to the internal infrastructure after a defined period of time has expired or on a given day without any intervention by the persons in charge of IT unless the period is renewed through access to the internal network. This methodology SHOULD be used as required as a preventive measure to ensure that the user is still in possession of the device.

SYS.3.2.3.A25 Using the Configuration Option for AirPrint (CI)

Approved AirPrint printers SHOULD be provided to the user by a configuration profile. In order to prevent information from being printed by the users on untrusted printers, it SHOULD be ensured that all communication links are always routed through the organisation's infrastructure systems.

SYS.3.2.3.A26 No Connections to Host Systems (CI)

To prevent iOS-based devices from being connected to other IT systems in an unauthorised manner, users SHOULD only be able to connect iOS-based devices to the MDM system.

Additional Information

For more information about threats and security safeguards for module SYS.3.2.3 iOS (for Enterprise), see the following publications, among others:

[ACSIOS]	iOS - Configuration recommendation based on operating system-internal means for use at increased levels of security: BSI publications on cyber security (BSI-CS 074), Version 1.20, December 2015 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_074.pdf , last accessed on 13.09.2018
[AppAGB]	Terms and Conditions for iTunes: Apple, https://www.apple.com/legal/internet-services/itunes/de/terms.html , last accessed on 13.09.2018
[AppAGBGC]	Terms and Conditions for Game Center : Apple, https://www.apple.com/legal/internet-services/itunes/gamecenter/de/terms.html , last accessed on 13.09.2018
[AppCon]	Apple Configurator: Apple, https://support.apple.com/de-de/apple-configurator , last accessed on 13.09.2018
[AppDS]	Apple Privacy Policy: Apple, https://www.apple.com/legal/privacy/de-ww/ , last accessed on 13.09.2018
[AppleSec]	Apple Security Updates: Apple Security Updates, https://support.apple.com/en-us/HT1222 , last accessed on 13.09.2018
[AppLPG]	Legal Process Guidelines: Apple, https://images.apple.com/legal/privacy/law-enforcement-guidelines-outside-us.pdf , last accessed on 13.09.2018
[AppViPro]	Vintage and Obsolete Products: Apple, https://support.apple.com/de-de/HT201624 , last accessed on 13.09.2018
[DEP]	Program for Device Registration: Find Apple Customer Numbers, Reseller IDs, and Organisation IDs, Apple, https://www.support.apple.com/de-de/HT6578 , last accessed on 13.09.2018
[Support]	Business and Education Support: Apple, https://www.apple.com/de/support/business-education/ , last accessed on 13.09.2018
[TR02102]	Cryptographic Mechanisms: Recommendations and Key Lengths: BSI TR-02102, Federal Office for Information Security (BSI), January 2018, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , last accessed on 13.09.2018
[VPP]	Volume Purchase Program: Apple, https://vpp.itunes.apple.com/de/store , last accessed on 13.09.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.3.2.3 *iOS (for Enterprise)*:

- G 0.9 Failure or Disruption of Communication Networks
- G 0.11 Failure or Disruption of Service Providers
- G 0.14 Interception of Information / Espionage
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.19 Disclosure of Sensitive Information
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.35 Coercion, Blackmail or Corruption
- G 0.36 Identity Theft
- G 0.37 Repudiation of Actions
- G 0.38 Misuse of Personal Information
- G 0.39 Malware
- G 0.41 Sabotage
- G 0.42 Social Engineering
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0. 9	G 0. 11	G 0. 14	G 0. 16	G 0. 19	G 0. 21	G 0. 22	G 0. 23	G 0. 25	G 0. 26	G 0. 27	G 0. 28	G 0. 29	G 0. 30	G 0. 32	G 0. 35	G 0. 36	G 0. 37	G 0. 38	G 0. 39	G 0. 41	G 0. 42	G 0. 46
SYS.3.2.3. A1			X	X	X	X	X	X	X			X	X	X	X			X	X		X		X
SYS.3.2.3. A2		X	X		X								X				X		X				X
SYS.3.2.3. A7					X	X	X	X						X	X	X		X	X		X		X
SYS.3.2.3. A10								X															
SYS.3.2.3. A11			X																				X
SYS.3.2.3. A12			X	X	X										X	X	X	X			X	X	X
SYS.3.2.3. A13			X	X	X	X	X	X		X		X	X	X	X		X	X	X		X	X	X
SYS.3.2.3. A14	X	X	X	X	X			X					X										
SYS.3.2.3. A15		X			X								X										X
SYS.3.2.3. A17			X	X	X	X	X	X							X		X						X
SYS.3.2.3. A18										X		X											
SYS.3.2.3. A20			X		X																X		X
SYS.3.2.3. A21			X		X	X			X	X		X			X						X	X	X
SYS.3.2.3. A23		X		X							X			X									



SYS.3.2.4: Android

Description

Introduction

Mobile devices are permanent companions in today's information society. They are always online, which means that they are connected to the Internet or the organisation's internal network, and thus offer access to digital information at all times. The devices may communicate via various interfaces, e.g. mobile radio, WLAN, or Bluetooth.

Due to their modern and simple control concepts and high performance, smartphones and tablets are very common nowadays. Originally, these devices were designed for private use. However, they are now also used within the occupational environment.

Android is a frequently used operating system for mobile phones. Starting with version 4, Android has been gradually implementing protections for business use. For example, functions that enable organisations to administrate Android devices have been integrated. The number of policies supported by Android also increases with every new version, and there are manufacturer-specific expansions that enable additional policies.

Objective

The objective of this module is to provide information on typical threats to Android-based devices and show how Android devices can be used securely in organisations. Moreover, security policies can be created on the basis of the requirements stated in the module.

Not in Scope

This module includes basic requirements which must be observed and fulfilled when operating Android-based devices. General and comprehensive requirements for the operation of smartphones and tablets are not part of this module; they are covered in module SYS.3.2.1 *General Smartphones and Tablets* and must also be implemented. Furthermore, requirements for the central administration of Android devices are not included in this module; they are listed in module SYS 3.2.3 *Mobile Device Management (MDM)*.

Threat Landscape

For module SYS.3.2.4 *Android*, the following specific threats and vulnerabilities are of particular importance:

Rooting Devices

Many of the previous versions of Android included vulnerabilities that made it possible to disable the security concept established by the manufacturer. Freely available tools exploit such vulnerabilities to grant super-user (root) rights to other apps.

Such apps may then access the data of the operating system and other apps. Malware also uses these vulnerabilities to manipulate the device or install itself on it. As a result, the operating system can be used for purposes other than those intended, and important security functions can be bypassed.

In particular, this affects access data that Android stores in protected areas because an app with super-user rights might be able to access the information stored there.

Malware for the Android Operating System

Due to their widespread use and open architecture, devices with the Android operating system are a popular target of malware. Since it is relatively easy in Android to install apps not only via the Google Play Store, but also via alternative stores or by direct download, the malware programs often use such methods to propagate themselves. An attacker could infect popular software with malware and then make it available for download.

Lack of Updates for the Android Operating System

Many manufacturers provide smartphones and tablets with outdated Android versions, fail to provide regular updates or provide no updates at all. Meanwhile, Android vulnerabilities are detected regularly, which poses a particular risk to such end devices. This problem mainly impacts low-cost devices and smaller manufacturers; however, larger manufacturers and premium models also often fail to provide a sufficient supply of security updates over the long term.

Concentration of Risk When One User Account (Google ID) Is Used for all Google Services

Users may use their Google ID for central access to all Google services, such as device management, recorded geographical locations, chat software, cloud storage, the Play Store, music, books, movies, backups, bookmarks, stored passwords for websites and synchronisation. Many other online service providers also use the Google ID for authenticating users.

If an attacker can use a Google ID for authentication, they may use such services with a stolen identity. The attacker also may access the data stored there, localise devices or reset them from a remote location (i.e. the attacker may delete all the data on the device).

Pre-Installed Apps and Integrated Functions on Android-Based Devices

Manufacturers often deliver deeply integrated and pre-installed apps (e.g. the Play Store and the corresponding Play Services) as well as interfaces for third-party services (Twitter, Facebook, etc) along with the operating system. In some cases, the user is not able to remove such apps. This increases the number of possible attacks on the Android operating system. The interfaces that cannot be deleted or configured are often not desired by the organisations.

Generally speaking, the deep integration of apps and third-party interfaces increases the risk of devices being infected with malware or attackers accessing devices without authorisation. This results in a lower level of data protection on the device.

Requirements

The specific requirements of module SYS.3.2.4 *Android* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	IT Operation Department
Further Roles	

Basic Requirements

For module SYS.3.2.4 *Android*, the following requirements **MUST** be implemented as a matter of priority:

SYS.3.2.4.A1 Selecting Android End Devices

When selecting an Android end device, it **MUST** be ensured that the manufacturer regularly provides security updates for the device. The end device **MUST** be delivered with an up-to-date version of Android or make it possible to update immediately to said version.

Standard Requirements

For module SYS.3.2.4 *Android*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

SYS.3.2.4.A2 Deactivating Developer Options

The developer options **SHOULD** be deactivated for all Android-based devices.

SYS.3.2.4.A3 Using the Multi-User and Guest Mode

It **SHOULD** be regulated whether the multi-user and guest mode may (or must) be used. A user on an Android-based device **SHOULD** correspond to a natural person.

SYS.3.2.4.A4 Rules for and Configuration of Cloud Print

Cloud Print **SHOULD** only be allowed if it is ensured that the user can only select approved printers.

SYS.3.2.4.A5 Advanced Security Settings

Only the approved security apps **SHOULD** be entered as device administrators or “Trust Agents”. This **SHOULD** be checked regularly by the security management.

Moreover, the settings for “Access to usage data and access to notifications” **SHOULD** only enable permitted apps to access this sensitive data.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.2.4 *Android* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.3.2.4.A6 Using a Malware Protection Product (CIA)

Software for protection against malware SHOULD be installed on Android-based devices. The software always SHOULD be up to date. Software SHOULD be used that has been rated as very good in independent tests.

SYS.3.2.4.A7 Additional Firewall (CI)

A firewall SHOULD be installed and activated on Android-based devices.

Additional Information

For more information about threats and security safeguards for module SYS.3.2.4 *Android*, see the following publications, among others:

[AN2]	2-Step Verification: Google, https://www.google.com/landing/2step/ , last accessed on 24.08.2018
[ANH]	Android Help: Google, https://support.google.com/android/?hl=de , last accessed on 24.08.2018
[ANL]	Overview of Android-Based Devices: Google, https://www.android.com , last accessed on 24.08.2018
[ANS]	Android Security Centre: Google, https://www.android.com/security/overview , last accessed on 24.08.2018
[ANU]	App Updates: Google, https://support.google.com/googleplay/answer/113412?hl=de , last accessed on 24.08.2018
[GAGB]	Google Terms of Service: October 2017, https://www.google.com/policies/terms/ , last accessed on 24.08.2018
[GPP]	Google Privacy Policy: October 2017, https://www.google.com/policies/privacy/ , last accessed on 05.10.2018
[GSUITE]	G Suite for Business and Education Support: Google, https://gsuite.google.com , last accessed on 05.10.2018
[TR21022]	Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths: Part 2: Use of Transport Layer Security (TLS), Federal Office for Information Security (BSI), January 2017, https://www.bsi.bund.de/DE/Publikationen/Technis-

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.3.2.4 *Android*:

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.21 Manipulation with Hardware or Software

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.41 Sabotage

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.14	G 0.16	G 0.21	G 0.28	G 0.30	G 0.32	G 0.38	G 0.39	G 0.41	G 0.46
SYS.3.2.4.A1				X				X		
SYS.3.2.4.A2	X		X			X			X	X
SYS.3.2.4.A3					X	X	X			
SYS.3.2.4.A4	X	X			X		X			X
SYS.3.2.4.A5					X					
SYS.3.2.4.A6	X		X					X		
SYS.3.2.4.A7	X		X					X		



SYS.3.3: Mobile Telephones

Description

Introduction

This module includes mobile telephones in accordance with the GSM standard (Global System for Mobile Communications), UMTS (Universal Mobile Telecommunications System) and LTE (Long Term Evolution).

The mobile phones considered in this module, also known as feature phones or "dumbphones", have fewer features than a smartphone, but offer more than just telephony. These mobile phones can also have a camera for videos and photos, an appointment calendar, e-mail programs, games, an MP3 player or a radio receiver. "Classic" mobile phones do not usually have a touch screen or an operating system on which apps can be installed. The lack of these functions distinguishes a conventional mobile phone from a smartphone.

Mobile phones are identified by an internationally unique serial number (IMEI). Mobile phone users are identified by their SIM cards, which are issued by mobile phone providers upon entry into a contract.

Objective

The aim of the module is to identify typical hazards that can occur when using mobile phones and to secure information stored on or transmitted by mobile phones.

Not in Scope

This module deals with general aspects of mobile phones, security aspects of telephony and messaging over the mobile network and how to use such devices. The module thus covers a wide range of different devices that can be connected to mobile telephone networks. Supplementary aspects that go beyond communication via a mobile network and handling related devices can be found in other modules of the IT-Grundschutz compendium.

Security requirements for smartphones and the operating systems used on them can be found in the SYS.3.2 *Tablets and Smartphones* module layer. Dedicated security properties such as those of mobile phone operating and display systems or specific hardware will not be described in more detail in this module. Aspects of IT-based telephony are covered in the module NET.4.2 *VoIP*. If a given mobile telephone uses VPN techniques, the module NET.3.3 *VPN* should also be considered.

Threat Landscape

For module SYS.3.3 *Mobile Telephones*, the following specific threats and vulnerabilities are of particular importance:

Inadequate Planning for the Purchase of Mobile Phones

If information on relevant features of the mobile phones to be purchased is not gathered during the planning phase, urgently required functions may not be available. In the worst case, the range of functions will not correspond to the intended purpose and render the devices entirely unusable. There are often additional general conditions that must be fulfilled to enable the use of devices. These include, for example, security features that are often not obvious at first glance, but can lead to availability and confidentiality issues when deployed.

Loss of a Mobile Phone

Since mobile phones are often small and are constantly carried around, they can easily be forgotten, lost or stolen. In addition to the economic damage, the loss of confidentiality and integrity of the data on the devices is particularly serious. An attacker may use a stolen mobile phone to access an organisation's confidential information. Costs and effort are also required to make the device usable again.

Carelessness in Handling Information

Employee inattentiveness and carelessness with mobile phones may allow third parties to access sensitive information. Information can be overheard or recorded during telephone conversations, and messages read as they are being written.

Unauthorised Private Use of a Mobile Business Phone

Mobile business phones can be used without permission for private purposes. Negligence and carelessness can cause major problems in terms of an organisation's information security – for example, when private and business content are mixed. If mobile business phones are used privately, additional costs may arise for the organisation.

Mobile Telephone Failure

There can be several reasons for mobile telephone failure. The user may fail to charge the device's battery or the battery may have lost its ability to stay charged. In addition, the user may have forgotten the access password or PIN and may no longer be able to use the device. Devices can also become locked if the access code is entered incorrectly several times. If the phone is not handled with care, it may become damaged when dropped, for example. In all of these instances, the user cannot be reached or contact others using the mobile phone.

Analysis of Call Data Relating to the Use of Mobile Phones

The inherent features of mobile communication mean it is impossible to prevent transmitted signals being listened to and recorded without permission by those willing to invest the effort. Due to technical reasons, connecting with mobile communication partners requires knowledge of their location when using most radio communication services. Location information can thus be used by network operators or service providers to create movement profiles.

Bugging of Meetings by Mobile Phones

Mobile phones can be used to record or listen to conversations unnoticed. If mobile phones are brought to meetings, they may be used to establish connections to unauthorised listeners. Many mobile phones are equipped with a speaker function that allows them to record conversations in the entire room with ease. Many devices do not make it obvious whether they are switched on or not, so it is not immediately apparent if calls are being recorded or listened to.

Use of Obsolete Mobile Phones

Since smartphones are more versatile than conventional mobile phones, many manufacturers exclusively offer smartphones. This means that the range of smartphones available clearly exceeds that of conventional mobile telephones; in fact, very few "dumbphones" are still produced. The low supply of conventional mobile phones encourages the use of mobile phones from old stocks. Old components such as batteries are often replaced by replicas from third-party manufacturers, allowing continued use of these mobile phones decades after production.

The operating systems installed on obsolete mobile phones are often outdated and no longer developed. It is no longer possible to eliminate software vulnerabilities by means of updates. The mobile phone manufacturer often no longer exists or has shifted its business to other markets. It is frequently impossible to purchase original accessories and spare parts, with even third-party manufacturers unable to offer corresponding products for very old mobile phones. Even if third-party manufacturers offer spare parts, there is no guarantee that these components will be of the same quality as the original parts (e.g. replicated batteries are often less efficient). It is often difficult to repair these devices or find a suitable contact person if the user requires help.

Requirements

The specific requirements of module SYS.3.3 *Mobile Telephones* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO), Human Resources Department, User, Supervisor

Basic Requirements

For module SYS.3.3 *Mobile Telephones*, the following requirements **MUST** be implemented as a matter of priority:

SYS.3.3.A1 Security policy and rules for the use of mobile telephones [Chief Information Security Officer (CISO)]

If mobile phones are used for business purposes, a usage and security policy **MUST** be established. Each mobile phone user **MUST** be provided with a copy of the security policy. Regular

checks **MUST** be carried out to ensure compliance with the security policy. The security policy on mobile phone use for business purposes **SHOULD** form part of the training on security safeguards.

SYS.3.3.A2 Blocking lost mobile telephones [User]

If a mobile phone is lost, the SIM card used in it **MUST** be blocked promptly. If possible, existing anti-theft mechanisms such as remote deletion or blocking **SHOULD** be used. All the information necessary to block the SIM card and mobile phone **MUST** be immediately at hand.

SYS.3.3.A3 Raising employees' awareness and providing training on the use of mobile telephones [Human Resources Department, Supervisor]

Employees **MUST** be made aware of the particular threats posed to information security by mobile phones. They **MUST** be familiar with the security features of mobile phones. Users **MUST** know the process of how to lock mobile phones. Mobile phone users **MUST** be advised of appropriate storage.

SYS.3.3.A4 Selection and proper disposal of mobile telephones and memory cards

Mobile phones **MUST** be reset to factory settings before disposal. A check **MUST** be carried out to confirm all data has been deleted. It **SHOULD** also be ensured that mobile phones and any memory cards are properly disposed of. If mobile phones and memory cards are disposed of at a later date or in larger quantities, the collected mobile phones and memory cards **MUST** be protected from unauthorised access.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module SYS.3.3 *Mobile Telephones*. They **SHOULD** be implemented as a matter of principle.

SYS.3.3.A5 Use of the security mechanisms of mobile telephones [User]

The available security mechanisms **SHOULD** be used and preconfigured on mobile phones. The SIM card **SHOULD** be protected by a secure PIN. The mobile phone **SHOULD** be protected by a device code. Where possible, the device **SHOULD** be reliant on the SIM card (SIM lock). The user **SHOULD** be informed about these security mechanisms.

SYS.3.3.A6 Mobile telephone updates [User]

Regular checks **SHOULD** be carried out to determine whether there are any software updates for the mobile phones. The handling of updates **SHOULD** be regulated. If there are new software updates, the way in which users will be informed about them **SHOULD** be specified. Whether users are allowed to install the updates themselves or the mobile phones are to be handed in at a central location for this purpose **SHOULD** be specified.

SYS.3.3.A7 Acquisition of mobile telephones

Before mobile phones components are acquired, a list of requirements **SHOULD** be created. The list of requirements **SHOULD** be used to evaluate the products available on the market. The product **SHOULD** be selected according to whether the manufacturers will offer updates for the planned period of use. It **SHOULD** be ensured that spare parts such as batteries and chargers can be procured in sufficient quality.

SYS.3.3.A8 Use of wireless interfaces [User]

IrDA, WLAN, Bluetooth and other wireless interfaces of mobile phones SHOULD be deactivated as long as they are not needed.

SYS.3.3.A9 Safeguarding the power supply [User]

Appropriate measures SHOULD be taken to ensure a sustainable supply of energy to mobile phones. The use of rechargeable batteries or power banks SHOULD be considered as required.

SYS.3.3.A10 Secure data transmission via mobile phones [User]

There SHOULD be rules defining the data which can be transmitted using mobile phones. The interfaces to be used SHOULD be defined. A decision SHOULD also be made on how to encrypt the data when necessary.

SYS.3.3.A11 Precautions for mobile telephones [User]

The data stored on a mobile phones SHOULD be backed up to another medium at regular intervals. If a defective mobile phone needs to be repaired, all data SHOULD be deleted and the device reset to the factory settings. Replacement devices SHOULD always be available to replace a failed mobile phone at short notice.

SYS.3.3.A12 Setting up a mobile telephone pool

Pooled storage SHOULD be set up if the users of business mobile phones change regularly. The issue and return of mobile phones and accessories SHOULD be documented. Before they are issued, it SHOULD be ensured that the mobile phones are charged and equipped with the programs and data the new owner will need. When mobile phones are issued, users SHOULD be informed about how to store them. In addition, users SHOULD be made aware of their obligation to comply with the relevant security policy. When devices are returned, they SHOULD be reset to factory settings.

Requirement in Case of Increased Protection Needs

Generic suggestions for module SYS.3.3 *Mobile Telephones* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account **IN THE EVENT OF INCREASED PROTECTION NEEDS**. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.3.3.A13 Protection against mobile telephone data being used to create movement profiles [User] (C)

It SHOULD be clarified whether the creation of movement profiles by third parties can have a negative effect or is regarded as a problem. To prevent GPS positioning, this function SHOULD be switched off. To prevent tracking through the mobile communication network, the mobile phone SHOULD be switched off and the battery removed.

SYS.3.3.A14 Protection against call number identification during use of mobile telephones [User] (C)

To prevent telephone numbers from being associated with specific people, numbers SHOULD be suppressed for outgoing calls and SMS or MMS messages SHOULD NOT be sent. Mobile phone numbers SHOULD NOT be published or passed on to unauthorised third parties.

SYS.3.3.A15 Protection against eavesdropping on indoor conversations using mobile tele-phones (C)

To ensure that sensitive information cannot be subject to eavesdropping, mobile phones SHOULD NOT be taken into rooms used for corresponding meetings and conversations. If necessary, this mobile phone ban SHOULD be enforced by detectors.

Additional Information

For more information about threats and security safeguards for module *SYS.3.3 Mobile Tele-phones*, see the following publications, among others:

[27001A6.2.1]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, in particular Annex A, A.6.2.1 Mobile device policy, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[NIST80053A C19]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, December 2014, https://nvd.nist.gov/800-53/Rev4/control/AC-19 , last accessed on 20.04.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module *SYS.3.3 Mobile Telephones*:

- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.17 Loss of Devices, Storage Media and Documents
- G 0.19 Disclosure of Sensitive Information
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.27 Lack of Resources
- G 0.29 Violation of Laws or Regulations
- G 0.31 Incorrect Use or Administration of Devices and Systems

Elementary Threats Requirements	G 0.14	G 0.15	G 0.16	G 0.17	G 0.19	G 0.22	G 0.23	G 0.25	G 0.27	G 0.29	G 0.31
SYS.3.3.A1	X	X			X	X			X		X
SYS.3.3.A2					X	X	X			X	
SYS.3.3.A3	X	X	X		X				X	X	X
SYS.3.3.A4	X	X	X	X	X					X	
SYS.3.3.A5	X				X	X					
SYS.3.3.A6											X
SYS.3.3.A7									X		
SYS.3.3.A8	X	X				X	X				
SYS.3.3.A9								X	X		
SYS.3.3.A10	X	X				X	X				
SYS.3.3.A11								X			
SYS.3.3.A12									X		
SYS.3.3.A13	X				X					X	
SYS.3.3.A14	X				X					X	
SYS.3.3.A15	X	X									



SYS.3.4: Mobile Storage Media

Description

Introduction

Mobile storage media are used for a large number of purposes – for example, to transport or store data or to use it on the go. There are a number of different versions of mobile storage media, including external hard disks, CD-ROMs, DVDs, memory cards, magnetic tapes and USB pen drives.

Storage media can be classified according to whether they are read-only, write-once or rewritable. They can also be divided according to other criteria, such as the type of data storage (analogue or digital), how they can be processed – without technical equipment (e.g. on paper) or only with technical equipment (e.g. DVDs) – and according to their design (removable storage media, external storage devices or storage media which are integrated into other devices).

Objective

This module shows how the information stored on mobile storage media can be used securely and how to prevent the unauthorised transfer of information via mobile storage media.

Not in Scope

This module only covers the basic security features of mobile storage media.

The protection of the IT systems to which the mobile storage media can be connected is not taken into account in this module. Recommendations for this can be found in the modules for the corresponding IT systems, such as SYS.1.1 *General Server* or SYS.2.1 *General Client*, as well as in the operating-system-specific modules.

The different and sometimes complex requirements for devices which can be used as mobile storage media in addition to their main function, such as smartphones and tablets, are provided in the modules covering the respective topics. Detailed aspects concerning the exchange of digital, but also analogue storage media are not considered either.

Mobile storage media can be exchanged in person or using transport services. The exchange of digital and analogue storage media to transmit information between different communication partners and IT systems is not considered in this module. The requirements of module OPS.1.2.3 *Exchange of Information and Storage Media* must be implemented in this regard.

Information on paper or other analogue storage media must also be taken into account in the security policy in addition to the digital storage media. These aspects go beyond the basic security features of mobile storage media and are thus covered in other modules (for example,

SYS.4.1 *Printers, Copiers, and All-in-One Devices*, NET.4.3 *Fax Machines and Fax Servers*, OPS.1.1.5 *Logging* or OPS.1.2.2 *Archiving*).

Threat Landscape

For module SYS.3.4 *Mobile Storage Media*, the following specific threats and vulnerabilities are of particular importance:

Carelessness in Handling Information

While many organisations have a number of organisational regulations and technical security procedures for mobile storage media, these are often then undermined through careless handling of the specifications and technology. It can regularly be observed, for example, that mobile storage media brought along by users are left unattended in meeting rooms during breaks or in train compartments.

Insufficient Knowledge of Rules and Procedures

If employees and those responsible for certain roles are not adequately familiar with the rules on the proper handling of mobile storage media, they cannot adhere to them either. Many threats to information security can occur, such as if USB pen drives are thoughtlessly connected to IT systems in the organisation.

Data Loss During Mobile Use

For mobile storage media, the risk of losing data is higher than for stationary systems. This can be due to theft or loss of the devices, but also to technical problems or a simple power outage. The information stored on the storage media is often irretrievably lost.

Defective Storage Media

Due to their size and fields of application, mobile storage media are prone to damage, errors and failures. This is caused, for example, by ever-changing operational environments or mechanical impacts.

Theft

Mobile storage media are stolen on a regular basis. The smaller and more popular such devices are (e.g. USB hard disks or pen drives), the higher the risk of them being stolen becomes. In addition to the material loss, further damage can occur if sensitive files are lost or disclosed.

Degradation Due to Changing Operating Conditions

Mobile storage media and devices are used in a very wide range of environments and are therefore subject to many threats. These threats include, for example, damaging environmental conditions such as excessively high or low temperatures, as well as dust and moisture. Other problems resulting from the portability of the devices include damage caused during transport. Another important aspect is that they are often used in areas which have different levels of security. Communicating with unknown IT systems and networks always poses a potential threat to one's own mobile end device. When the storage media are connected to other IT systems, confidential information which is not intended to be disclosed can also be copied (for example).

Spreading of Malware

Mobile storage media are often used to exchange data between different devices and the workplace. Here, there is the risk that malware will infect the mobile storage media and thus spread to the workplace systems.

Data Theft Using Mobile Storage Media

Mobile storage media such as USB pen drives or memory cards are mostly small, discreet and high in capacity. Since almost all IT systems are equipped with a corresponding interface for removable storage media, there is the risk that large amounts of data can be copied in an unauthorised manner without attracting attention.

Requirements

The specific requirements of module SYS.3.4 *Mobile Storage Media* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	IT Operation Department
Further Roles	User, Process Owner

Basic Requirements

For module SYS.3.4 *Mobile Storage Media*, the following requirements **MUST** be implemented as a matter of priority:

SYS.3.4.A1 Raising Staff Awareness of Secure Handling of Mobile Storage Media

All employees **MUST** be made aware of how to handle mobile storage media in a secure manner. The employees **MUST** also be instructed in the careful handling of mobile storage media to prevent their loss or theft, but also to guarantee a long service life.

SYS.3.4.A2 Reporting the Loss of Mobile Storage Media [User]

It **MUST** be reported immediately if a mobile storage medium used for official purposes is lost or stolen. This **SHOULD** also apply to private storage media used for official purposes. There **SHOULD** be clear reporting paths and contact persons in every organisation for this purpose.

SYS.3.4.A3 Backup Copies of Transferred Data [User]

If the data to be transferred on a mobile storage medium has only been created or collected specifically for transfer and is not stored on any other storage medium, a backup copy of this data **MUST** be made.

Standard Requirements

For module SYS.3.4 *Mobile Storage Media*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.3.4.A4 Drawing Up a Policy for the Secure Handling of Mobile Storage Media [User]

A policy defining how mobile storage media are to be handled SHOULD be drawn up. The following essential aspects SHOULD be taken into account:

- which mobile storage media may actually be used and who is allowed to use them
- which data may be stored on mobile storage media
- how the data stored on the mobile storage media will be protected against unauthorised access, tampering and loss
- how the data on the mobile storage media is to be deleted
- whether and how private storage media are allowed to be used
- the external employees or service providers with whom storage media may be exchanged and which security regulations are to be observed
- how to prevent the mobile storage media from being used to disclose information without authorisation
- how to prevent the spread of malware via mobile storage media

Furthermore, it SHOULD be regulated how private mobile storage media may be used in the organisation. Moreover, it SHOULD be checked at regular intervals whether the security specifications for handling mobile storage media are still up to date.

SYS.3.4.A5 Rules Regarding the Transportation of Mobile Storage Media

There SHOULD be clear written rules defining whether and how the mobile storage media may be transported. In particular, these rules SHOULD define which storage media may be transported out of the office, who is allowed to transport them out of the office and which basic security safeguards have to be observed (virus protection, encryption of sensitive information, storage, etc). The users SHOULD be informed of the rules.

SYS.3.4.A6 Storage Media Management [Process Owner]

Mobile storage media SHOULD be managed in a well-regulated manner. Inventory lists SHOULD be kept. To achieve this, the storage media SHOULD be labelled in a standardised manner. Moreover, it SHOULD be ensured as part of managing storage media that mobile storage media are appropriately handled and stored as well as properly used and transported.

SYS.3.4.A7 Secure Deletion of Storage Media Before and After Use [Process Owner]

Before rewritable storage media are passed on for further use or disposed of, they SHOULD be deleted appropriately.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.3.4 *Mobile Storage Media* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate the key security objectives which are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.3.4.A10 Encryption of Storage Media (C)

In case of high protection needs, mobile storage media SHOULD always be encrypted completely whenever possible even if they are only occasionally used for confidential information. A secure encryption algorithm SHOULD be used. In order to meet the confidentiality requirements of the information to be transmitted, corresponding encryption programs SHOULD be installed on the sender's and the recipient's IT system.

SYS.3.4.A11 Protecting Integrity Using Checksums or Digital Signatures (I)

In order to ensure only the integrity of confidential information when exchanging data by means of mobile storage media, a procedure for protecting the data against accidental or deliberate changes SHOULD be used. Examples include checksum procedures, error-correcting codes, message authentication code (MAC) or digital signatures. The procedures for the protection against changes SHOULD conform to the current state of the art.

Additional Information

For more information about threats and security safeguards for module SYS.3.4 *Mobile Storage Media*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[NIST800150]	Guide to Cyber Threat Information Sharing: Special Publication 800-150, October 2016, http://dx.doi.org/10.6028/NIST.SP.800-150 , last accessed on 05.10.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.3.4 *Mobile Storage Media*:

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.3 Water

G 0.4 Pollution, Dust, Corrosion

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.1	G 0.2	G 0.3	G 0.4	G 0.1 4	G 0.1 6	G 0.1 7	G 0.1 9	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 4	G 0.2 5	G 0.2 6	G 0.2 9	G 0.3 0	G 0.3 8	G 0.3 9	G 0.4 1	G 0.4 2	G 0.4 5	G 0.4 6
SYS.3.4.A1	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SYS.3.4.A2					X					X								X				X
SYS.3.4.A3						X	X	X														X
SYS.3.4.A4	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SYS.3.4.A5	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SYS.3.4.A6	X	X	X	X	X	X	X	X	X			X	X	X		X	X					X
SYS.3.4.A7					X	X	X	X									X	X		X		X
SYS.3.4.A10					X	X	X	X	X	X	X				X		X		X	X	X	X
SYS.3.4.A11					X	X	X	X	X	X							X		X	X	X	X



SYS.4.1: Printers, Copiers, and All-in-One Devices

Description

Introduction

Printers, copiers, all-in-one devices and scanners are often servers with their own operating system and mechanical components. Since these devices often process confidential information, they must be protected along with the entire print and scan infrastructure.

Paper is still used as an information carrier for many business processes, which makes printers and all-in-one devices important components in the IT infrastructure. If the devices fail, this can sometimes affect critical processes and lead to considerable economic damage.

Objective

This module describes how printers, scanners, copiers and all-in-one devices can be operated safely so that information is not extracted from them and the security of the rest of the internal IT infrastructure is not impaired.

Not in Scope

This module deals with the security of printers and all-in-one devices, as well as the specific elements of the IT infrastructure. Networked document scanners are not explicitly covered, but the risks and requirements are similar to those for all-in-one devices. Networked fax machines are also not considered separately. The risks and requirements listed in this module for fax functions also apply to this type of device and should be taken into account along with the requirements of module NET.4.3 *Fax Machines and Fax Servers*.

Print servers are systems with print queues, print job management and possible other components, such as driver distribution or secure printing. For each print server, the general and operating-system-specific security requirements for servers must be implemented. These are described not in this module, but in module SYS.1.1 General Server and the respective operating-system-specific server modules.

Threat Landscape

For module SYS.4.1 *Printers, Copiers, and All-in-One Devices*, the following specific threats and vulnerabilities are of particular importance:

Unauthorised Access to Printed Documents

Printed documents can often remain in the output tray of central printers and all-in-one devices for an extended period of time, such as when users first print out several files and then collect them all together or they have selected the wrong printer on the workstation computer and cannot find their documents at the expected location. Since floor or department printers are used by many users, unauthorised persons can also view sensitive information or take it with them.

However, there are even risks involved when printouts are left behind in the output trays of decentralised workplace printers located in the offices of the users. Anyone who can enter the office where a workplace printer is located could also view or remove the printouts.

Fax documents and printed transmission logs in the output tray pose a further risk; in addition to the fax number, date, time and page number, they often contain a scaled-down image of the first page. Since such logs are only output after a fax has been sent or a transmission error has occurred, they can sometimes remain lying around for a longer period of time or not be picked up at all. This means that confidential information is left unattended in the output tray of the device and can be stolen, for example.

Uncollected documents will also eventually be disposed of by users. In a great many cases, the printed information is not protected in the process (e.g. the printouts are simply thrown into unsecured waste paper bins). This means that sensitive information can reach the public waste disposal system and thus fall into the hands of third parties.

Many home workstations are equipped with a printer or an all-in-one device. Most organisations do not regulate how users should dispose of confidential documents, which could allow sensitive information to be disclosed.

Visibility of Metadata

A print job usually includes metadata that contains the user ID, date, time, and the name of the print job. This data is displayed on the control panel and web server of many printers and all-in-one devices. The name of the print job is often derived from the name of the digital document. Users can therefore view confidential information using a browser and by entering the hostname or IP address of any device in the organisation. The metadata is also visible in plain text on the print servers unless it is anonymised, which could allow third parties to obtain confidential information. Many devices also allow print jobs to be saved so that they can be printed out later after authentication with a PIN. This is another case in which the name of all available documents is displayed on the control panel of an output device.

Some printers and copiers print “yellow dots” (also referred to as machine identification code, tracking dots or secret dots) on the paper. These often undocumented watermarks, which may include the date, time, and the serial number of the printer, are hardly visible to the naked eye. This way, a printout may be associated directly with an organisation or even a certain user, making it possible to trace the printout back to its author. In addition to the consequences regarding data protection laws, information might accidentally leave the organisation.

Fax logs can also be printed without access protection on many all-in-one devices. Even if they only list the telephone number, date, time and number of pages, conclusions can be drawn about personal or business transactions.

Insufficient Protection of Stored Information

Printers and all-in-one devices are often equipped with non-volatile storage on which information is stored temporarily or for longer periods of time. For example, address books, documents, fax files and print jobs are stored there. If this information is not adequately protected, attackers can access it and read it. In some cases, attackers can even reconstruct information that has already been deleted. This is possible if unsafe deletion methods were used.

Data can be stored and read in the device via network protocols. Printers and all-in-one devices with hard disks or SSDs can often be used as unauthorised file servers if they are not secured. In this way, uncontrolled information that is not taken into account in the backup concept can be stored in a decentralised manner.

Unencrypted Communication

Print and scan data is often transmitted in unencrypted form in the network. This allows an attacker to intercept transmitted documents. Print files that are temporarily stored in print servers can also be read. The same applies to central scanning and document processing systems.

Unencrypted communication interfaces for device administration are also a source of risk. If, for example, printers are accessed via HTTP, SNMPv2 or Telnet, the information is not protected when it is transmitted. This endangers the access information, including device passwords.

Unauthorised Sending of Information

Many all-in-one devices can send digitised paper documents by e-mail and fax. Without special precautions, these functions can deliberately or accidentally transmit information to unauthorised recipients. Users can often enter recipient addresses or telephone numbers incorrectly, for example. As a result, personal data may be unintentionally sent to the wrong recipient. In addition, attackers can use the e-mail or fax function to quickly send confidential documents to the outside world.

Many networked printers can be configured to receive print jobs from the Internet via e-mail and send scanned documents as e-mail attachments. The user-defined input field for the sender's e-mail address can be misused to send e-mails under a different name to internal and external recipients. Even if the artificial machine name is entered as the sender and this cannot be changed, the apparently authorised sender will still appear as the address of the organisation.

Unauthorised Copying and Scanning of Information

Documents on paper can be quickly copied using all-in-one devices. Existing USB or SD ports also make it possible to digitise even large quantities of paper documents directly and without any controls, store them on USB pen drives or SD cards and take them away unnoticed.

No Network Separation

Firewalls between a LAN and the Internet are often configured such that Internet access is enabled for entire subnets. On the other hand, printers and all-in-one devices are often assigned to the same subnet as the workstation PCs. This means it is also possible for the network printers, for example, to access the Internet. If the connections from the Internet to the printers are not rejected by the security gateways, this can allow sensitive information to leak from the network without permission under some circumstances. By the same token, a network-capable

printer could also receive and distribute unwanted data from the Internet. A network printer may therefore become an opening for attacks from the Internet.

Poor Access Protection for Device Administration

Networked printers and all-in-one devices can be managed from the control panel and built-in web server. When the devices are delivered, they usually have no or only one manufacturer-specific default password. If the password is not set or not changed, the devices can be accessed very easily.

Many organisations also use common passwords for all printers and all-in-one devices, which are rarely changed. As a result, they are often known to many internal and external persons, which makes it easy for unauthorised third parties to access the devices.

In addition, printers and all-in-one devices can be reset to factory settings via boot menus. This also affects the security settings: for example, the device password often no longer exists after the printer or all-in-one device has been reset to the factory settings. Unprotected boot menus simplify administration, but reduce security at the same time.

Printers and all-in-one devices are equipped with numerous network protocols. All protocols are usually activated on delivery. This could allow attackers, for example, to access the device settings and modify them to extract sensitive information from the network.

Many devices can transfer their control panel to a support representative via the network. However, this can also be used to read confidential entries made by users on the control panel of the device.

There are usually many printers and all-in-one devices in larger organisations. Device management software is often used to manage and monitor them efficiently. Many organisations do not adequately protect device management software from unauthorised access because it is perceived as a less critical system. This central approach allows individual or all devices to be changed unintentionally or deliberately.

Manipulation of the Operating System

If the operating system is insufficiently protected by printers and all-in-one devices, attackers can manipulate it. This makes it possible for information to be sent out undetected or for the systems to be misused for unwanted activities.

Requirements

The specific requirements of module SYS.4.1 *Printers, Copiers, and All-in-One Devices* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) and Data Protection Officer must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO),

	Head of IT
--	------------

Basic Requirements

For module SYS.4.1 *Printers, Copiers, and All-in-One Devices*, the following requirements MUST be implemented as a matter of priority:

SYS.4.1.A1 Drawing Up a Basic Concept for the Use of Printers, Copiers, and All-in-One Devices [Head of IT]

Before printers, copiers and all-in-one devices are procured, a basic concept MUST be drawn up for their secure use. In this concept, it MUST be regulated where the devices are allowed to be placed, who may access them and how they are to be protected against attacks.

SYS.4.1.A2 Suitable Siting and Access to Printers, Copiers and All-in-One Devices

Printers and all-in-one devices MUST be set up, configured and secured so that only authorised users can use the devices and access processed information. In addition, it MUST be ensured that only authorised persons can administer, maintain and repair the devices. Confidentiality agreements MUST be made in writing with service providers (e.g. for maintenance).

Printers, copiers and all-in-one devices MUST be provided with device passwords to block access from the web server and control panel. The password MAY ONLY be known to authorised users and MUST be changed regularly.

Unused device functions SHOULD be switched off.

SYS.4.1.A3 Regularly Updating Printers, Copiers, and All-in-One Devices

It MUST be checked at regular intervals whether printers, copiers and all-in-one devices are up to date. If vulnerabilities are identified, these MUST be eliminated as soon as possible. Existing patches and updates MUST be installed immediately or, if there are no patches, other security safeguards MUST be implemented. It MUST be ensured in general that patches and updates are only obtained from trustworthy sources.

SYS.4.1.A12 Correct Disposal of Devices and Sensitive Resources

Before the organisation disposes of or returns old devices, all sensitive data on the devices MUST be securely deleted. If this is not possible, the mass storage system SHOULD be removed and destroyed by suitable processes. Service providers commissioned with the disposal MUST be obliged to comply with the necessary security measures.

Unused but printed documents with sensitive information MUST be disposed of in an appropriate manner (e.g. in suitable paper containers). Suitable rules SHOULD also be put in place for home workstations.

Standard Requirements

For module SYS.4.1 *Printers, Copiers, and All-in-One Devices*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.4.1.A4 Drawing Up a Security Concept for the Use of Printers, Copiers and All-in-One Devices [Head of IT]

The persons in charge SHOULD draw up a security concept for printers and all-in-one devices. It SHOULD regulate the requirements and specifications for the information security of the devices and how these are to be met. It SHOULD also specify which functions may be administered or used by which users under which conditions.

SYS.4.1.A5 Drawing Up User and Administration Policies for Handling Printers, Copiers, and All-in-One Devices [Chief Information Security Officer (CISO)]

An administration policy SHOULD be drawn up for the secure handling of printers, copiers and all-in-one devices. An instruction sheet SHOULD also be created for users in which all safety requirements for handling printers and all-in-one devices are clearly and comprehensibly summarised. The instruction sheet SHOULD be familiar to all users.

SYS.4.1.A7 Restriction of Remote Administrative Access to Printers, Copiers, and All-in-One devices

Only a clearly defined group of administrators and service technicians SHOULD be allowed remote administrative access to printers, copiers and all-in-one devices. This SHOULD also be ensured if the organisation uses central device management software.

It SHOULD be specified whether the control panel display can be viewed via a data network. If this is desired, it SHOULD only be transferable to employees in the IT Operation Department. This SHOULD also be agreed with the users concerned.

SYS.4.1.A11 Restricting the Connection of Printers, Copiers, and All-in-One Devices

Network printers and all-in-one devices SHOULD NOT be accessible from external networks. When connecting all-in-one devices to the telephone network, it SHOULD be ensured that no uncontrolled data connections can be established between the organisation's data network and the telephone network.

SYS.4.1.A15 Encryption of Information for Printers, Copiers, and All-in-One Devices

If possible, all information stored on internal non-volatile storage media (e.g. hard disks, SSDs) SHOULD be encrypted. Print jobs SHOULD be transmitted in an encrypted form if possible.

SYS.4.1.A17 Protection of the Payload and Metadata

Payload data such as print jobs and scan files SHOULD only be stored on the devices for as short a time as possible. The data SHOULD be deleted automatically after a specified time. Device-based file servers and functions such as "*Scan to device memory*" SHOULD be disabled. The protocols and functions required for this SHOULD be blocked whenever possible.

In general, care SHOULD be taken to ensure that all metadata (e.g. of print jobs) is not visible to unauthorised persons. It SHOULD be regulated how printouts with metadata are to be passed on to third parties.

SYS.4.1.A18 Configuration of Printers, Copiers and All-in-One Devices

All printers and all-in-one devices SHOULD be configured in line with a defined security policy.

The devices SHOULD be managed exclusively via encrypted protocols such as HTTPS and SNMPv3. All protocols that allow unencrypted access to printers and all-in-one devices SHOULD be replaced by encrypted ones and switched off. This should be implemented in particular for protocols that can be used to change the device configuration (e.g. SNMP, Telnet, PJI). The default *SNMP Set Community Name* SHOULD be changed.

SYS.4.1.A19 Secure Deletion of Information on Printers, Copiers and All-in-One Devices

It SHOULD be ensured that deleted data cannot be reconstructed. Released data segments SHOULD be overwritten automatically with random values. All cryptographic keys and certificates that are no longer required SHOULD be securely deleted.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.4.1 *Printers, Copiers, and All-in-One Devices* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.4.1.A14 Authentication and Authorisation for Printers and All-in-One Devices (CI)

Only authorised persons SHOULD be able to access the printed or copied documents.

If possible, only central printers and all-in-one devices that require prior user authentication SHOULD be used. Only the functions necessary for the respective user SHOULD be enabled. After the users have authenticated themselves, only their own print jobs SHOULD be visible.

SYS.4.1.A16 Contingency Planning for Printers, Copiers and All-in-One Devices (A)

The downtime of printers, copiers, and all-in-one devices SHOULD be kept to a minimum. Among other measures, the following SHOULD therefore be taken:

- Replacement devices should be made available.
- An appropriate response time should be ensured in maintenance contracts.
- A list of specialised suppliers should be maintained in order to be able to quickly purchase replacement devices or spare parts.
- A store of regularly required spare parts should be maintained if necessary.

SYS.4.1.A20 Enhanced Information Protection for Printers, Copiers and All-in-One Devices (C)

Print files with confidential information SHOULD only be transmitted in encrypted form. The names of the print jobs SHOULD also only be displayed anonymously on the print server.

All interfaces for external storage media SHOULD be disabled.

Furthermore, device-internal address books SHOULD be deactivated and alternative addressing methods (e.g. address search via LDAP) offered to users.

Printers and all-in-one devices with e-mail functionality SHOULD ensure that e-mails can only be sent using the e-mail address of an authenticated user. Documents SHOULD also only be sent to internal e-mail addresses. Alternatively, the devices SHOULD be set so that scanned documents can only be sent to a fixed address that has been entered.

Incoming fax documents and transmission reports SHOULD only be accessible to authorised users.

SYS.4.1.A21 Extended Protection of Printers and All-in-One Devices (IA)

The security settings of printers and all-in-one devices must be regularly checked and corrected as necessary. If an automated control and correction system is available, it SHOULD be used.

In addition, there SHOULD be a restriction on the devices being reset to the factory settings via the boot menu. It SHOULD be ensured that no firmware or additional software can be installed on printers and all-in-one devices that has not been verified and approved by the respective manufacturer.

Additional Information

For more information about threats and security safeguards for module SYS.4.1 *Printers, Copiers, and All-in-One Devices*, see the following publications, among others:

[ACSD]	Whitepaper Datenschutz und Sicherheit in Druckinfrastrukturen [White Paper on Data protection and security in print infrastructures]: mc ² management consulting GmbH, May 2018, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/230518_mc2_sichere_druckinfrastrukturen.html , last accessed on 05.07.2018
[CERT]	Information about vulnerabilities and security gaps of printers and related services, warning and information service of CERT-Bund: CERT-Bund, https://www.cert-bund.de/search , last accessed on 05.07.2018
[CSE015]	Drucker und Multifunktionsgeräte im Netzwerk [Printers and all-in-one devices in the network]: BSI publications on cyber security (BSI-CS 015), Version 1.1., February 2017, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_015.html , last accessed on 15.11.2017
[CSE069]	Sichere Passwörter in Embedded Devices: Verhinderung von Schwachstellen durch Standardpasswörter und festcodierten Zugangsdaten [Secure passwords in embedded devices: preventing vulnerabilities with standard passwords and hard-coded access data]: BSI publications on cyber security: (BSI-CS 069), Version 1.0, December 2013, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_069.html , last accessed on 05.07.2018
[NIST80053PE5]	NIST Special Publication 800-53: NIST Special Publication 800-53, Revision 4, April 2013, in particular PE-5 Access control for output devices, http://nvlpubs.nist.gov/nist-pubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 05.07.2018
[PP0058]	IEEE Standard Protection Profile for Hardcopy Devices in IEEE Std 2600-2008: Operational Environment B, IEEE Std 2600.2-2009, IEEE Computer Society, Information As-

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.4.1 *Printers, Copiers, and All-in-One Devices*:

G 0.14 Interception of Information / Espionage

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.39 Malware

Elementary Threats Requirements	G 0.14	G 0.16	G 0.18	G 0.19	G 0.21	G 0.23	G 0.25	G 0.30	G 0.32	G 0.39
SYS.4.1.A1	X	X	X	X	X	X	X			
SYS.4.1.A2	X	X		X	X	X				
SYS.4.1.A3					X		X			X
SYS.4.1.A4	X	X	X	X		X		X	X	
SYS.4.1.A5	X			X				X	X	
SYS.4.1.A7	X			X	X	X		X	X	
SYS.4.1.A11				X		X		X		X
SYS.4.1.A12	X			X						
SYS.4.1.A14	X			X	X	X		X	X	X
SYS.4.1.A15	X			X						
SYS.4.1.A16							X			
SYS.4.1.A17	X			X						
SYS.4.1.A18	X			X	X	X		X	X	
SYS.4.1.A19	X			X						
SYS.4.1.A20	X				X	X		X	X	
SYS.4.1.A21					X	X				



SYS.4.3: Embedded Systems

Description

Introduction

Embedded systems are information-processing systems which are integrated into a larger system or product; assume control, regulation and data processing tasks there; and are often not recognised directly by the user. Embedded systems can be found both in the field of advanced technology – such as aerospace, medical engineering, telecommunications and automotive engineering – and in the consumer and household appliances sector.

An embedded system is characterised by the fact that it consists of software and hardware that forms a functional unit and performs only one defined task. The software of embedded systems is referred to as firmware and is, in most cases, stored in flash memory, EPROM, EEPROM or ROM. It can either not be exchanged by the user at all, or only with special means or functions. It mainly consists of the boot loader, the operating system and the application, with specialised systems doing without an operating system. Although embedded systems are specialised devices, they are universal computers in contrast to pure hardware implementations (ASIC). Different CPU architectures or flexible, highly integrated Field Programmable Gate Array (FPGA) components can be used as platforms.

Embedded systems either have no user interface or use special peripheral equipment, such as functional keys, rotary switches and displays designed for the respective intended purpose. The scope of output units ranges from a simple signal lamp to LCDs and complex cockpit displays. Embedded systems frequently communicate via data buses which are networked heterogeneously in complex systems. In addition, peripheral components such as sensors and actuators can be connected via several different and multi-channel input/output ports. Some types of embedded systems are equipped with a web interface via which configuration settings can be made using a browser.

Objective

The objective of the module is to provide information on typical threats to embedded systems and show how these systems can be used securely in organisations.

Not in Scope

This module deals with embedded systems in general. It should be applicable to a wide range of different embedded systems. Dedicated security properties, such as those of operating and display systems or specific hardware and software architectures, will not be described in more detail here. Likewise, the security aspects of embedded systems used in industrial control systems are not specifically addressed. The IND layer modules (*Industrial IT*) are intended for this

purpose. Specific security aspects of IoT systems are not part of this module either. They are covered in *SYS.4.4 General IoT Devices*.

Chip cards are a special application of embedded systems. The cards are usually equipped with a processor, random access memory and I/O interfaces. This module covers the general security aspects relating to chip cards, but not the specific aspects.

Threat Landscape

For module *SYS.4.3 Embedded Systems*, the following specific threats and vulnerabilities are of particular importance:

Inadequate Security Requirements for Developing Embedded Systems

For cost reasons, information security often plays a less important role during the development of embedded systems than, for example, performance or reliability. However, if security requirements are not sufficiently addressed in one or more development phases, the embedded systems may have serious vulnerabilities.

Unprotected Input/Output Interfaces in Embedded Systems

The interfaces in embedded systems are potential points of attack. This applies to interfaces on all levels of the ISO/OSI layer model and all transmission media used. If access via the interfaces is not controlled or if the control mechanisms are too weak, attackers could infiltrate the system, read and write data without authorisation and initiate subsequent attacks. They could connect spying or sabotage devices unnoticed, such as miniaturised controllers or data loggers. If such devices are connected to the I/O ports at the microcontroller level, signals could be fed into the I/O registers via the I/O lines or output signals could be recorded. If there is a reset input, attackers could control it and temporarily shut down the system.

Inadequate Physical Protection for Embedded Systems

If embedded systems are easy to access physically, attackers could destroy or damage the systems, e.g. by mechanical force, short circuits or excess voltage. They could also access the electronic components, e.g. IC pins or contacts, and thus record the electrical signals unnoticed with corresponding measuring and analysis tools, or feed in signals themselves. When attackers gain possession of an embedded system, they can use physical procedures to read and manipulate data or access data that has not been securely deleted. This may result in the confidentiality, integrity or availability of the information stored on the embedded system being compromised.

Hardware Failure and Hardware Errors with Embedded Systems

Environmental influences such as electromagnetic interference, temperature fluctuations, an unstable power supply, manufacturing defects and production tolerances, or normal or premature wear can cause embedded systems to fail. This could cause them to malfunction and severely affect the adjacent systems.

Installation (Flashing) of Manipulated Software Updates with Embedded Systems

Many embedded systems store their software on flash memory or EEPROM and provide the ability to update their firmware by connecting a programming device via a data interface or network connection. However, an attacker can also use this to import manipulated software

updates and thus change how a system functions. The original tasks of the system can thus be interrupted or manipulated.

Side-Channel Attacks on Embedded Systems

Attackers could use a side-channel attack to break encryptions or signatures by exploiting observable properties of the physical implementation of a cryptosystem. For example, they could use the energy consumption of a microprocessor during cryptological calculations to draw conclusions about related keys and the operations being carried out. They could also conduct computational timing attacks, microarchitectural attacks or (semi-)invasive attacks. In 2011, scientists could identify the secret key of a TLS/SSL server that was using the Digital Signature Algorithm (DSA) with elliptic-curve cryptography. The attack was based on the fact that the time required for multiplication makes it possible to draw conclusions about the corresponding operands.

Entry and Manipulation via the Communication Interface of Embedded Systems

Embedded systems are often limited with regard to code size, time behaviour, energy consumption and size and weight. They are thus often not equipped with sufficient security functions such as strong cryptography. However, modern embedded systems are increasingly interconnected by widespread techniques and protocols, and are therefore potentially vulnerable.

Attackers may try to manipulate data or software on an embedded system by abusing the default communication interfaces and protocols for their own purposes. If the IP communication or Ethernet, WLAN, Bluetooth and mobile or digital radio interfaces are not sufficiently secured, for example, an attacker may take over connections, forge messages, or enter a system and perform subsequent attacks. Furthermore, an attacker can also try to enter the system using other available communication interfaces, e.g. USB ports.

Use of Forged Components

During the production process or when components are replaced during servicing, forged components may be installed in embedded systems. Since counterfeits of many components are in circulation, this can also happen unintentionally. Forged components are often less reliable than the original components, which could cause functions to fail or work incorrectly. Attackers may also develop a device or component that looks exactly the same as the original, but contains manipulated functions. Such components could create backdoors, manipulate individual functions, or reduce availability, for example.

Requirements

The specific requirements of module *SYS.4.3 Embedded Systems* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
---------------------	-------------------------

Further Roles	Procurement Agent, Planner, Developer, Head of IT
----------------------	---------------------------------------------------

Basic Requirements

For module SYS.4.3 *Embedded Systems*, the following requirements **MUST** be implemented as a matter of priority:

SYS.4.3.A1 Provisions for the use of embedded systems [Head of IT]

A person **MUST** be appointed to be in charge of embedded systems in order for them to operate smoothly. All users and administrators **MUST** be informed of behavioural rules and reporting channels in the event of failures, malfunctions or suspected security incidents. Users and administrators **SHOULD** be sufficiently trained in the use of the respective embedded system.

Embedded systems **MUST** be securely preconfigured and their configuration **SHOULD** be documented. Regulations **SHOULD** be defined for testing integrity and functionality.

SYS.4.3.A2 Deactivating unused interfaces and services with embedded systems [Developer]

It **MUST** be ensured that only required interfaces are available. Only the required services **MAY** be activated. Access to the application interfaces **MUST** be protected by means of secure authentication.

SYS.4.3.A3 Logging security-relevant events for embedded systems

Security breaches **MUST** be logged (see OPS.1.1.5 *Logging*). If electronic logging is not feasible or only possible to a very limited extent, organisational rules **SHOULD** be created and implemented.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module SYS.4.3 *Embedded Systems*. They **SHOULD** be implemented as a matter of principle.

SYS.4.3.A4 Procurement criteria for embedded systems [Procurement Agent, Head of IT]

Before an embedded system is procured, a requirements list **MUST** be drawn up that can be used to evaluate the systems or components available on the market. The requirements list **SHOULD** include the following security-relevant aspects:

- aspects of material security
- requirements for the security properties of the hardware
- requirements for the security properties of the software
- security aspects of the development environment
- organisational security aspects

SYS.4.3.A5 Protection against damaging environmental influences with embedded systems [Developer, Planner]

It SHOULD be ensured that embedded systems are adequately protected from harmful environmental influences according to their intended use and location. The requirements for this SHOULD be analysed right from the planning phase. It SHOULD also be ensured that the precautions taken to protect individual components from dust and contamination are compatible with the requirements of the generic system.

SYS.4.3.A6 Preventing debugging options for embedded systems [Developer]

Possible debugging options SHOULD be removed from embedded systems as completely as possible. If on-chip debugging is used, it MUST be ensured that debugging functions cannot be used or activated by unauthorised persons.

It SHOULD also be ensured that no input interfaces for test signals and measuring points for the connection of analysers can be activated or used by unauthorised persons. All hardware debugging interfaces SHOULD also be disabled.

SYS.4.3.A7 Hardware realisation of the features of embedded systems [Developer, Planner, Procurement Agent]

If embedded systems are developed in-house, security aspects SHOULD be taken into account in the design decision for hardware and software implementation. Security aspects SHOULD also be taken into account when deciding to implement a particular hardware technology.

SYS.4.3.A8 Secure operating system for embedded systems [Developer, Planner, Procurement Agent]

The operating system used and the configuration of the embedded system SHOULD be suitable for the intended operation. The operating system SHOULD thus have sufficient security mechanisms for the intended task. The required services and functions SHOULD be activated. The operating system SHOULD support the use of a Trusted Platform Module (TPM).

SYS.4.3.A9 Use of cryptographic processors or coprocessors in embedded systems [Developer, Planner, Procurement Agent]

If an additional microcontroller is used for cryptographic calculations, its communication with the system microcontroller SHOULD be adequately secured. The required trust anchors SHOULD be realised for the embedded system. A chain of trust SHOULD also be implemented.

SYS.4.3.A10 Recovery of embedded systems

Embedded systems SHOULD have rollback capabilities.

SYS.4.3.A11 Secure disposal of embedded systems [Head of IT]

All data on the system SHOULD be securely deleted before the disposal of embedded systems. The deletion or destruction SHOULD be documented.

Requirement in Case of Increased Protection Needs

Generic suggestions for module SYS.4.3 *Embedded Systems* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a

risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.4.3.A12 Selection of a trustworthy supplier and logistics chain and a qualified manufacturer for embedded systems [Procurement Agent, Head of IT] (CI)

Effective controls SHOULD be carried out in the logistics chain to ensure that

- the embedded system does not include any manipulated, falsified, or replaced components
- the system meets the specification and no hidden functions have been implemented during manufacture
- confidential information on the embedded system cannot be accessed by unauthorised persons

The companies involved SHOULD be demonstrably qualified.

SYS.4.3.A13 Use of a certified operating system [Developer, Planner, Procurement Agent] (CI)

The operating system SHOULD be evaluated with respect to a recognised standard on an adequate level.

SYS.4.3.A14 Secured and authenticated boot process for embedded systems [Developer, Planner, Procurement Agent] (CI)

The boot process of an embedded system SHOULD be secured by the boot loader based on its ability to check the integrity of the operating system and only load it when it is classified as correct. Conversely, the operating system SHOULD also check the integrity of the boot loader.

A multi-stage boot concept SHOULD be used that can check the individual steps in a cryptographically secure manner. A secure hardware trust anchor SHOULD also be used. ARM Secure Boot SHOULD be used in an ARM-based embedded system. Secure Boot SHOULD be used with a Unified Extensible Firmware Interface (UEFI).

SYS.4.3.A15 Storage protection in embedded systems [Developer, Planner, Procurement Agent] (CI)

Memory protection mechanisms SHOULD be considered right from the design of embedded systems. The type of storage protection and the number and size of the protected areas SHOULD be appropriate for the purpose.

SYS.4.3.A16 Tamper protection for embedded systems [Planner] (CI)

A tamper protection concept SHOULD be developed for embedded systems. Adequate mechanisms SHOULD be established to detect, record and prevent tamper attacks. Adequate guidelines SHOULD also be established on how to respond to a tamper attack.

SYS.4.3.A17 Automatic monitoring of the assembly function [Planner, Procurement Agent] (IA)

All the assemblies of an embedded system with higher requirements for availability and integrity SHOULD be equipped with integrated self-test equipment (built-in self-test, BIST). Tests SHOULD check the integrity of the system during the switch-on process and at adequate time

intervals during operation. Where possible, the self-test functions SHOULD also check security functions and security properties of the assembly.

The integrity of the memory and I/O components SHOULD be checked regularly within the framework of the BIST. Existing BIST functions SHOULD be supplemented by the required functions if possible.

SYS.4.3.A18 Resistance of embedded systems to side-channel attacks [Developer, Procurement Agent] (C)

To make embedded systems resistant to side-channel attacks, appropriate precautions SHOULD be taken against non-invasive and (semi-)invasive side-channel attacks.

Additional Information

For more information about threats and security safeguards for module “SYS.4.3 *Embedded Systems*”, see the following publications, among others:

[ICSSK]	ICS Security Compendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten [Test recommendations and requirements for component manufacturers], Federal Office for Information Security (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html , last accessed on 05.10.2018
[ICSSKfH]	ICS Security Compendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten, Federal Office for Information Security (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.4.3 *Embedded Systems*:

G 0.4 Pollution, Dust, Corrosion

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.37 Repudiation of Actions

G 0.39 Malware

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.4	G 0.1 5	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 4	G 0.2 5	G 0.2 6	G 0.2 8	G 0.2 9	G 0.3 0	G 0.3 1	G 0.3 7	G 0.3 9	G 0.4 6
SYS.4.3.A1			X										X		X			
SYS.4.3.A2								X						X				
SYS.4.3.A3						X	X	X		X	X			X		X		
SYS.4.3.A4			X		X													
SYS.4.3.A5	X									X								
SYS.4.3.A6								X						X				
SYS.4.3.A7						X	X	X	X									
SYS.4.3.A8		X			X	X	X	X					X					X
SYS.4.3.A9		X				X	X	X										X
SYS.4.3.A10										X					X			
SYS.4.3.A11		X		X														
SYS.4.3.A12	X		X		X	X	X							X				
SYS.4.3.A13		X			X	X	X	X					X					X
SYS.4.3.A14						X	X							X			X	
SYS.4.3.A15						X	X										X	
SYS.4.3.A16						X	X		X						X			
SYS.4.3.A17						X	X			X	X							X
SYS.4.3.A18		X				X												X



SYS.4.4: General IoT Devices

Description

Introduction

In this module, devices with functionalities from the field of the Internet of Things (IoT) are considered. As opposed to “classic” IT systems, these are intelligent objects that also include “smart” features. IoT devices are normally connected to data networks (wirelessly in many cases), and they can often even access the Internet and be accessed in the same way. As a consequence, they may have effects on the information security of the entire information domain.

IoT devices may exist in organisations because they are brought along by employees or external persons (e.g. smartwatches or wearables). However, IoT devices are also procured and operated in many organisations – as, for example, in the case of fire, gas and other warning detectors; coffee machines; or building management elements such as cameras and HVAC (heating, ventilation and air conditioning) systems.

In general, a differentiation may be made between IoT devices that may be addressed directly and IoT devices that require a central controller. Devices that can be addressed directly are usually connected to a data network with their own IP address and can act autonomously, or are managed by a central control unit. However, there also are IoT devices that communicate only directly with controllers (e.g. via radio networks such as Bluetooth or ZigBee) and thus do not connect directly to data networks. The coverage of these radio connections may, if provided, be increased by means of a separate, intermeshed network wherein each device establishes a radio connection to every other device.

Objective

The objective of this module is to secure IoT devices such that they impair neither the security of the information and IT of one’s own organisation nor the security of external parties. As a consequence, both non-authorized data leaks and any manipulation of the devices should be avoided, especially with regard to attacks on third parties.

Not in Scope

This module addresses IoT devices in general and should thus be applicable to a wide range of IoT devices. Dedicated security properties such as those of operating and display systems or specific hardware and software architectures will not be described in more detail here.

Depending on the characteristics of the IoT devices, their interfaces to industrial control systems (ICS systems) or embedded systems may be fluid. Requirements for devices used in the field of production and manufacturing can be found in the modules of the IND layer (industrial IT).

Embedded systems are information-processing systems which are integrated into a larger system or product, where they assume control, regulation and data processing tasks and are often not recognised directly by the user. Module *SYS.4.3 Embedded Systems* must be implemented for these systems.

Requirements for the radio links often used in this context can be found in the modules of the layer *NET.2 Radio Networks*.

Threat Landscape

The following specific threats and vulnerabilities are of particular importance for module *SYS.4.4 General IoT Devices*:

Espionage Using IoT Devices

When developing IoT devices, the aspect of information security is typically a secondary development objective (if it is considered at all). As a consequence, it has often been possible to misuse IoT devices to collect information on the users and the field of use. For example, there have been repeated incidents in connection with networked and IP-based surveillance cameras:

- In 2013, several banks in different countries were compromised using their surveillance cameras during the “Carbanak” campaign. The attackers obtained hundreds of millions. Within the framework of these attacks, the cameras were used to capture screen contents and keyboard input in the banks.
- In 2014, the Insecam website was used in order to publicly disclose the video images and streams of 73,000 poorly protected webcams.
- In 2015, the Conficker malware (which was already eight years old at the time) infected numerous bodycams of different police officers.

Use of UPnP

IoT devices integrated into LANs often automatically establish a connection to the Internet by configuring routers in the network using UPnP (universal plug-and-play) to facilitate port forwarding. In this case, the devices are not only able to communicate with the local network; they are both visible and even available from outside of the LAN. If an attacker exploits a vulnerability in the IoT devices in this case, the device might become part of a bot network. It is also possible that additional malware will be incorporated into the information domain. This gap could theoretically be used for other activities at a later point in time.

Damage Involving Third Parties

If IoT devices are not patched at regular intervals, known vulnerabilities remain open and may be used for extensive attacks. One objective of an attack may be to integrate IoT devices into a bot network. In this case, they might be used to execute DDoS attacks (distributed denial of service) and restrict the availability of services, for example.

Example: At the end of October 2016, a DDoS attack was carried out on an Internet service provider using a botnet which consisted largely of IoT devices. Due to the large number of devices, the so-called Mirai bot network reached a bandwidth that vastly exceeded the previously known bot networks. The webcams, cameras, DVR players, routers and printers that were

already part of the bot network automatically scanned the Internet for further devices in order to infect them with malware and add them to the bot network.

Espionage Attacks by Means of Backdoors in IoT Devices

At the end of September 2016, it became known that some models of surveillance cameras and room sensors had backdoors that allowed for espionage. In particular, this affected surveillance cameras used in data centres and server rooms. The backdoors apparently made it possible to access the image and video data of the cameras and copy this data to servers on the Internet. In this way, user and administration passwords may be compromised or device configurations, infrastructure details and other confidential information may be made available to third parties, for example. This facilitates more comprehensive attacks by exploiting the habits of the personnel.

Requirements

The specific requirements of module *SYS.4.4 General IoT Devices* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO), Procurement Department, Building Services

Basic Requirements

For module *SYS.4.4 General IoT Devices*, the following requirements **MUST** be implemented as a matter of priority:

SYS.4.4.A1 Criteria for Using IoT Devices

IoT devices **MUST** meet minimum security criteria before being used in organisations. The devices **MUST** have update features and the manufacturer **MUST** offer an update process. The devices **MUST** allow for authentication. Hard-coded access data **MUST NOT** be present on the device.

SYS.4.4.A2 Authentication

In order to use an IoT device in an organisation, authentication **MUST** be enabled. If passwords are used in this regard, they **MUST** be secure. A password policy **SHOULD** be in place. These passwords **MUST** be sufficiently complex, kept secret and changed at regular intervals. Preset passwords **MUST** be changed. In addition, the use of alternative mechanisms such as certificate-based authentication is recommended.

SYS.4.4.A3 Regular Updates

It **MUST** be checked at regular intervals whether the IoT devices and the related components (such as sensors or management systems) are up to date. If vulnerabilities are identified, these

MUST be eliminated as soon as possible. Existing patches and updates MUST be installed immediately or, if there are no patches, other security safeguards MUST be implemented. It MUST be ensured in general that patches and updates are only obtained from trustworthy sources.

SYS.4.4.A4 Activation of Automatic Update Mechanisms

Automatic update mechanisms MUST be activated unless other mechanisms (such as regular manual maintenance or a central software distribution system) are used for updates. If a time interval can be specified for auto-update mechanisms, there SHOULD be an automatic search for updates at least daily and they SHOULD be installed if found.

SYS.4.4.A5 Restriction of Network Access

Network access of IoT devices MUST be restricted to the required minimum and controlled. This includes the following:

- traffic control at network gateways, e.g. by means of rules on firewalls and access control lists (ACLs) on routers only previously defined incoming and outgoing connections may be admissible
- restrictive configuration of routing on IoT devices and sensors, particularly the suppression of default routers
- signatures on intrusion prevention systems (IPS)
- the IoT devices and sensors SHOULD be operated in a separate network segment that is only allowed to communicate with the network segment for management
- configuration of virtual private networks (VPNs) between the networks with IoT devices and sensor networks and management networks
- the UPnP feature MUST be disabled on all routers

Standard Requirements

For module SYS.4.4 *General IoT Devices*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

SYS.4.4.A6 Integration of IoT Devices into the Security Policy of the Organisation

In the general security policy of the organisation, the requirements for IoT devices SHOULD be specified. The policy SHOULD be known to all persons involved in the procurement and operation of IoT devices, and must form the foundation of their work. The implementation of the rules required by the policy SHOULD be reviewed regularly and the results should be documented in a sensible way.

SYS.4.4.A7 Planning the Use of IoT Devices

For secure operation of IoT devices, it SHOULD be planned in advance where and how these should be used. This planning SHOULD address not only aspects associated with information security in a traditional sense, but also normal operational aspects that entail requirements in the area of security. Specifications for authentication, update mechanisms and network connections SHOULD be defined. All decisions made in the planning phase SHOULD be documented such that they can be understood at any given future point in time.

SYS.4.4.A8 Procurement Criteria for IoT Devices [Procurement Department, Chief Information Security Officer (CISO)] (I)

The CISO SHOULD also be involved in procuring devices that do not have any obvious IT functionality. Prior to procuring IoT devices, the security requirements they must meet SHOULD be specified. When procuring IoT devices, aspects of material security and requirements regarding the security characteristics of the software SHOULD be sufficiently considered. A requirements list SHOULD be drawn up that can be used to evaluate the products available on the market. IoT devices with a cloud concept SHOULD not be procured.

SYS.4.4.A9 Controlling the Use of IoT Devices

A person SHOULD be put in charge of the operation of every IoT device. The persons in charge SHOULD be informed sufficiently regarding the way the IoT device should be handled. All the persons in charge, users, and administrators SHOULD be informed of behavioural rules and reporting channels for failures, malfunctions and suspected security incidents.

SYS.4.4.A10 Secure Installation and Configuration of IoT Devices

The framework conditions applicable to the installation and configuration of IoT devices SHOULD be defined. Installation and configuration of the IoT devices SHOULD only be performed by authorised persons (persons in charge of IoT devices, administrators or service providers bound by contracts) in accordance with a defined process. All installation and configuration steps SHOULD be documented such that the installation and configuration can be understood and repeated by a qualified third party based on the documentation.

The basic settings of IoT devices SHOULD be checked and, where necessary, adapted to the specifications of the security policy. If possible, IoT devices SHOULD only be connected to IT networks after installation and configuration are complete; this is particularly applicable to public networks.

SYS.4.4.A11 Use of Secure Protocols

Data SHOULD only be transmitted in an encrypted form. IoT devices SHOULD support a protocol that is based on encryption (e.g. SSL/TLS or SSH). If the product itself does not offer any encryption, this SHOULD be implemented additionally during commissioning (e.g. using a virtual private network, VPN).

SYS.4.4.A12 Secure Integration into Superior Systems [Chief Information Security Officer (CISO)] (I)

If IoT devices are being used in connection with superior management systems, they SHOULD only communicate with these management systems.

SYS.4.4.A13 Deactivation and Uninstallation of Unnecessary Components

Upon completion of the installation, it SHOULD be checked which protocols, applications and other tools are installed and enabled on the IoT devices. Protocols, services, user IDs and interfaces that are not required SHOULD be disabled or uninstalled entirely. This applies in particular to insecure services such as Telnet or SNMPv1/v2. The use of radio interfaces that are not required (e.g. for WLAN, ZigBee, or Bluetooth) SHOULD be prevented.

If this is not possible using the device itself, services that are not required SHOULD be restricted using the security gateway (firewall). The decisions taken SHOULD be documented such that it can be understood which configuration was selected for the IoT devices.

SYS.4.4.A14 Approval for Use

Prior to making production use of IoT devices and connecting them to a production network, they SHOULD be approved for use. This SHOULD be documented. For the purposes of approval, the installation and configuration documentation and the functionality of the IoT devices SHOULD be tested. This SHOULD be performed by an entity authorised for this purpose within the organisation.

SYS.4.4.A15 Restrictive Granting of Access Rights

The access authorisations for IoT devices SHOULD be granted as restrictively as possible. If this is not possible using the IoT devices themselves, it SHOULD be considered via the network.

SYS.4.4.A16 Elimination of Malware on IoT Devices

The IT Operation Department SHOULD regularly obtain information as to whether the IoT devices used may become infected with malware and how this malware may be removed. Malware SHOULD be eliminated immediately. If the cause of the infection cannot be eliminated or a new infection cannot be effectively prevented, the affected IoT devices SHOULD no longer be used.

SYS.4.4.A17 Monitoring the Network Traffic of IoT Devices

It SHOULD be monitored whether there is network traffic from the IoT devices or sensor systems to non-management systems.

SYS.4.4.A18 Logging Security-Relevant Events on IoT Devices

Security-relevant events SHOULD be logged automatically. If this is not possible using the IoT devices themselves, routers and other logging mechanisms SHOULD be used. The logs SHOULD be evaluated to a reasonable extent.

SYS.4.4.A19 Protection of Administration Interfaces

Depending on whether IoT devices are administered locally; directly using the network; or using central, network-based tools, appropriate security precautions SHOULD be taken. The methods used for administration SHOULD be defined in the security policy. The IoT devices SHOULD be administered according to the security policy. Administration via the network SHOULD be performed via secure protocols.

SYS.4.4.A20 Controlled Decommissioning of IoT Devices

When decommissioning IoT devices, it SHOULD be ensured that no important data that might still be present on their storage media is lost and that no sensitive data remains. There SHOULD be an overview of the data stored in each location on IoT devices. A checklist which can be completed when decommissioning IoT devices SHOULD be created. This checklist SHOULD, at minimum, include aspects of backing up data that is still needed and the subsequent secure deletion of all data.

Requirements in Case of Increased Protection Needs

Generic suggestions for module SYS.4.4 *General IoT Devices* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

SYS.4.4.A21 Operational Environment and Power Supply [Building Services, Chief Information Security Officer (CISO)] (I)

It SHOULD be clarified whether IoT devices may be operated in the intended operational environment (i.e. taking the protection needs of other systems and data protection into account). IoT devices SHOULD be protected against theft, destruction and manipulation in the operational environment.

It SHOULD be clarified whether an IoT device has certain requirements regarding the physical operational environment (e.g. humidity, temperature, energy supply). If required, additional safeguards SHOULD be implemented regarding the infrastructure.

If IoT devices are operated using batteries, a procedure SHOULD be specified for regular functional testing and replacement of the batteries.

IoT devices SHOULD be protected against dust and pollution in accordance with their intended type and place of use.

SYS.4.4.A22 System Monitoring (A)

The IoT devices SHOULD be integrated into a suitable system monitoring concept which continuously monitors the system status and the functionality of the IoT devices while reporting error conditions and exceeded thresholds to the operating personnel. If the IoT devices have high availability requirements, it SHOULD be checked whether the devices used meet these requirements and whether additional measures (such as the configuration of a cluster or the procurement of standby devices) are necessary.

SYS.4.4.A23 Auditing of IoT Devices (CIA)

In security-critical areas, all IoT devices used SHOULD be inspected from a security point of view by experts.

SYS.4.4.A24 Secure Configuration and Usage of an Embedded Web Server (CIA)

Web servers integrated into IoT devices SHOULD be configured as restrictively as possible. Only the components and functions required SHOULD be installed and activated. The web server SHOULD NOT be operated using a privileged account if this can be avoided. Security-relevant events SHOULD be logged. Access MAY ONLY be possible after successful authentication. The transmission SHOULD be encrypted.

Additional Information

For more information about threats and security safeguards for module SYS.4.4 *General IoT Devices*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[ACS1]	Security of IP-based surveillance cameras: BSI publications on cyber security (BSI-CS 128), Version 1.1, November 2016, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_128.html , last accessed on 15.11.2017

[ACS2]	Spionageangriffe mittels Hintertüren in Überwachungskameras und Raumsensoren: So schützen Sie Ihr Unternehmen, Expertenkreis Cyber-Sicherheit, [Spy attacks using back doors in surveillance cameras and room sensors: How to protect your business, Cyber Security Expert Group], October 2016 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/partner/161010_expkr_statement01.pdf , last accessed on 05.10.2018
[DHS]	Securing the Internet of Things: Department of Homeland Security (DHS), November 2016, https://www.dhs.gov/securingtheIoT , last accessed on 05.10.2018
[OWASP]	Open Web Application Security Project (OWASP): https://www.owasp.org , last accessed on 05.10.2018

Appendix: Cross-reference Table for Elementary Threats

The following Elementary Threats are relevant for module SYS.4.4 *General IoT Devices*:

- G 0.2 Unfavourable Climatic Conditions
- G 0.4 Pollution, Dust, Corrosion
- G 0.8 Failure or Disruption of the Power Supply
- G 0.9 Failure or Disruption of Communication Networks
- G 0.14 Interception of Information / Espionage
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.23 Unauthorised Access to IT Systems
- G 0.24 Destruction of Devices or Storage Media
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems

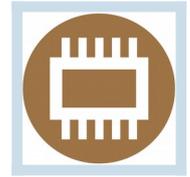
G 0.38 Misuse of Personal Information

G 0.39 Malware

G 0.40 Denial of Service

Elementary Threats Requirements	G 0.2	G 0.4	G 0.8	G 0.9	G 0.1 4	G 0.1 6	G 0.1 8	G 0.1 9	G 0.2 0	G 0.2 1	G 0.2 3	G 0.2 4	G 0.2 5	G 0.2 6	G 0.2 8	G 0.2 9	G 0.3 0	G 0.3 8	G 0.3 9	G 0.4 0
SYS.4.4.A1					X		X	X	X		X			X	X					
SYS.4.4.A2					X			X		X	X						X	X	X	X
SYS.4.4.A3					X		X	X	X	X	X		X	X	X		X	X	X	X
SYS.4.4.A4					X		X	X	X	X	X		X	X	X		X	X	X	X
SYS.4.4.A5					X			X	X	X	X		X	X	X	X	X	X	X	X
SYS.4.4.A6	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
SYS.4.4.A7	X	X	X	X		X	X	X		X	X						X	X	X	X
SYS.4.4.A8					X		X		X		X			X	X					
SYS.4.4.A9	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X					
SYS.4.4.A10					X		X	X		X	X		X		X		X	X	X	X
SYS.4.4.A11					X					X				X		X	X	X	X	X
SYS.4.4.A12				X	X		X									X				
SYS.4.4.A13					X			X		X	X			X	X		X	X	X	X
SYS.4.4.A14							X		X								X			
SYS.4.4.A15					X			X		X	X			X		X	X	X	X	X
SYS.4.4.A16																			X	
SYS.4.4.A17				X	X					X	X		X	X	X		X			X

SYS.4.4.A1 8				X		X		X	X					X			
SYS.4.4.A1 9				X		X		X	X			X		X	X	X	X
SYS.4.4.A2 0						X	X										
SYS.4.4.A2 1	X	X	X		X	X				X	X		X				
SYS.4.4.A2 2								X	X		X	X					X
SYS.4.4.A2 3				X		X	X	X	X			X	X				
SYS.4.4.A2 4				X		X			X			X		X			



IND.1: Operational and Control Technology

Description

Introduction

Operational technology (OT) is hardware and software which records and causes changes by directly monitoring or controlling physical devices, processes and events in the company [GART1].

In the industrial realm – which also includes critical infrastructures – this particularly refers to industrial control systems (ICS) and automation solutions which handle control and closed-loop control functions of all kinds. Other examples include laboratory equipment (e.g. automated microscopes or analysis tools), logistics systems (barcode scanners with microcomputers) or building management systems.

The physical separation of OT from other IT systems and networks in office applications, which was common in the past, can today only be applied in exceptional cases in the case of elevated protection needs due to increasing integration requirements. Multi-stage production steps and the overarching control thereof are, along with regulatory requirements, making an increasingly open approach necessary, including across organisational boundaries. This development is being accelerated by the trend towards the optimisation of production processes in order to increase competitiveness within the scope of Industry 4.0.

Since IT components and technologies of office IT are increasingly being used in OT in addition to OT-specific components, they have become exposed to comparable threats. At the same time, OT differs considerably from conventional IT, which makes it difficult to apply the established security procedures from the latter field. There can be restrictions due to manufacturer specifications or legal requirements which prevent or hinder changes to components. The application of security updates or subsequent hardening measures are two examples. In addition, OT is usually subject to significantly longer lifecycles (even beyond the manufacturer support provided), which means that the continuing availability of security updates can also not be ensured.

OT also presents an essential difference in terms of the high availability and integrity requirements that are often involved, whereas confidentiality is frequently of secondary importance compared to office IT. Malfunctions of these systems can result in hazards to life, limb and the environment, and they cannot be remedied by a restart in most cases.

Objective

The objective of this module is to present appropriate requirements for the information security of OT. It addresses cross-component, design-related and architectural security requirements.

The module must be modelled and implemented comprehensively. Multiple uses in different areas of the OT in an organisation (operators within the meaning of VDI 2182) cannot be ruled out, as these areas are subject to different requirements with respect to information security.

Not in Scope

Even in comparable use cases, the design of OT can vary greatly depending on the purpose, industry, IT systems and technology used, as well as due to the long period of use (without updates, in some cases) of such technology. When designing the security safeguards on the basis of the requirements from this module, the existing particularities must therefore be taken into account. They can significantly influence the design of the security concept. For this reason, the risk analysis can already be very important when drawing up a security concept for normal protection needs. The module may thus need to be used several times for different areas.

In addition, the surrounding infrastructure of the OT (e.g. sites, systems, buildings and rooms) must be modelled by modules which are as suitable as possible for the subject at hand in order to complement the protective effect of this module.

Threat Landscape

For module IND.1 *Operational and Control Technology*, the following specific threats and vulnerabilities are of particular importance:

Inappropriate Integration of OT into the Security Organisation

Different framework conditions, knowledge and procedures in the fields of office IT and ICS can cause implementation problems in the case of comprehensive security specifications. On the one hand, security specifications from the area of IT may not be implemented due to technical or procedural particularities of ICS systems. On the other hand, the persons in charge of office IT information security may not be familiar with ICS-specific information security and safety aspects (aspects of functional security). This can result in friction in communication and implementation, as well as in risks which are not treated adequately or not detected.

Inappropriate Integration of OT into Operating Procedures

Irrespective of the increasing convergence of OT and IT, there are particularities which make it difficult to transfer established operating procedures. Operational interventions as part of the change and (security) incident management for the secure configuration, troubleshooting or installation of security updates, for example, can entail another official approval or the loss of manufacturer support. Unauthorised changes can influence the functioning of a component and thus potentially also impact its safety functions.

OT is used to monitor, control and automate technical processes. Malfunctions of these systems can lead to losses of production or damage to technical equipment, personnel or the environment. These potential impacts must be taken into consideration regarding operational interventions.

Inappropriate Access Protection

Industrial control systems that are operated without any connection to the outside world are becoming increasingly rare. Modern manufacturing and production processes require an exchange of information with upstream and downstream production steps and are often connected to central production planning and control systems (manufacturing execution systems/enterprise resource planning) of an organisation. The electronic exchange of information requires that production systems be connected to other networks (such as for office IT), including those of partners and service providers. Requirements related to interactive access from office or mobile workplaces – as well as operational requirements for the electronic exchange of data, such as the provision of software and updates or the realisation of remote access for on-call service or service providers – are driving connectivity with the outside world.

If the required communication channels are too wide-ranging or inadequately secured, attackers may use them to gain network-based access and compromise the automation system.

Inadequate Protection Concept Against Malware for OT

Industrial control systems can be affected by both targeted malware attacks and randomly by malware that aims to compromise office IT. Possible paths of infection result from data transfers, the use of removable media and mobile end devices or a lack of segmentation or control of data traffic.

On the other hand, using anti-virus software can also pose risks for OT if there is no manufacturer approval for the environment in question or error detections and active system interventions jeopardise operations. Comparable potential for disruption (caused by the interruption of connections) can also result from the operation of network-based intrusion prevention systems (IPS).

When using anti-virus software, regular updates are also required. If this is not ensured, new attacks using malware will not be detected. This also generally applies to attacks for which the anti-virus software does not have signatures.

Insecure Project Planning Process/Application Development Process

Adjustments and further developments of IT systems, applications and control programs represent critical interventions in the control system. Malfunctions can arise from functional errors in the case of inadequate test and validation steps, incorrect or manipulated project planning data or vulnerabilities in the software if important security functions (such as input and output or authorisation checks) are implemented inadequately.

Other threats can result from insecure development environments or unsuitable storage of program code, documentation or project data, as well as from the data transfer interfaces.

Insecure Administration Concept and Remote Administration

The administration of industrial control systems is performed in certain cases via network access. In this respect, different public and private networks are used, such as telephone networks, radio networks, mobile networks and, in more and more cases, the Internet. If such access is planned inadequately, configured insecurely or not monitored, attackers might be able to access individual OT components or the infrastructure in an unauthorised manner under certain circumstances and thus bypass the security mechanisms at the perimeter.

Local administrators are also equipped with privileged rights, which makes misusing them an attractive option for internal attackers or external attackers (via compromised accounts).

Inadequate Monitoring and Detection Procedures

Monitoring of the operational conditions of the process to be automated is an essential function of industrial control systems. Warnings concerning the process (e.g. if fill levels are not met) and technical parameters (e.g. temperatures, valve positions) are usually shown. At the same time, however, the monitoring of the supporting IT infrastructure is often inadequate.

If unusual or security-relevant events of such operational environments are inadequately monitored (or not at all), attempted attacks, network bottlenecks or foreseeable failures cannot be detected at an early stage.

Moreover, poor evaluation or confusing presentation of the events may also lead to warnings and errors being detected too late.

Inadequate Test Concept

Industrial control systems are often subject to high availability requirements. Under certain circumstances, malfunctions or technical failures might result in serious damage and high consequential costs. For this reason, systems are often designed to be fail-safe and redundant.

If changes to such an environment are not carefully planned, coordinated and tested in a realistic environment, there is the risk that logical or software-related errors will be overlooked and malfunctions will occur in the system. Even updates released by the manufacturer can cause malfunctions in the system when modifications are made or parameters adjusted.

Lack of Lifecycle Concepts

In addition to specific OT components, components, technologies and software from office IT ("commercial off-the-shelf" (COTS) products) are seeing increasing use. Due to the very long lifecycles in OT, these components are usually operated much longer than is common in office IT – even beyond the support cycles provided by product suppliers in some cases.

As a result, updates for vulnerabilities are no longer provided after the supplier's support has expired. Meanwhile, there are often publicly documented vulnerabilities and tools available to exploit them. This makes it possible for even inexperienced attackers to successfully enter the systems. The same applies if updates are not installed or installed only with a very long delay.

Furthermore, the long periods of use can cause problems when procuring spare parts if they are no longer produced by the manufacturer. This may also apply to knowledge regarding the care and maintenance of legacy systems, which new employees will not have.

Use of Insecure Protocols

The OT components communicate with each other using different network protocols and technologies. ICS-specific protocols are used in addition to protocols and technologies from the area of office IT (e.g. Ethernet, TCP/ IP, WLAN, GSM). Not all of these elements have been developed from the point of view of information security, and some thus offer limited security mechanisms (or none at all). Information is frequently transmitted as plain text without securing the integrity or without authentication.

An attacker with access to the network could read or change the contents of the communication and thus influence the processes – for example, by faking sensor data or forging control commands. This applies in particular to protocols which are used for communication via freely accessible areas, such as for radio protocols or as part of location networking (remote control technology).

Insecure Configurations

In the default configuration of OT components, security safeguards are not always activated, which means that it is significantly easier to gain unauthorised access. The operation of insecurely configured components can also be a threat to the security of other components of the environment, such as when access data regarding these components can be read or the components are in a trust relationship with other systems.

Examples of insecure configurations include the use of default passwords, the use of plain text protocols for system administration, the operation of unnecessary services, unprotected interfaces such as USB or FireWire ports and deactivated security functions.

Dependencies Between OT and IT Networks

Today, OT is operated less and less often in a completely independent environment. If there are dependencies with other systems, networks or services, failures or security incidents in the IT network might also affect OT.

In particular, if these systems and networks are not under the control of the organisation (the operator of the ICS infrastructure), this may lead to severe adverse effects on production and the availability of OT and processes. Furthermore, a given incident or error can usually only be remedied with external support.

Example of dependencies with other systems and networks include Internet connections (whether using a cable connection or a mobile link), shared infrastructure components, operational management and monitoring by service providers and the increasing use of cloud services.

Requirements

The specific requirements of module IND.1 *Operational and Control Technology* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	ICS Information Security Officer
Further Roles	IT Operation Department, Area Security Officer

Basic Requirements

For module IND.1 Operational and Control Technology, the following requirements **MUST** be implemented as a matter of priority:

IND.1.A1 Integration into the Security Organisation

An information security management system (ISMS) for the operation of the OT infrastructure **MUST** either be an independent ISMS or part of an overall ISMS and, in its scope of application, **MUST** explicitly include the definition of objectives and values, processes, roles, responsibilities and specifications for OT.

The top management level of the organisation **MUST** initiate, control and monitor the security process. The organisation **MUST** establish a security organisation which manages the roles and responsibilities for the information security of the OT infrastructure and components.

A person in charge of overall information security in the field of OT **MUST** be designated and announced within the organisation. Legal, regulatory and other special specifications for the field of OT and for the respective industry or sector **MUST** be known and their effects on the organisation evaluated.

There **MUST** be a process that determines how concrete specifications (policies) for specific topics in the process area are to be drawn up, communicated, implemented, updated, assessed and improved.

Additional information is described in module ISMS.1 *Security Management*.

IND.1.A2 Awareness and Training of Personnel

The operating personnel **MUST** be informed about relevant IT security threats in the field of OT at regular intervals and have their awareness raised in this respect. The persons in charge of OT **MUST** be informed or trained regarding the threat landscape and need for action at regular intervals.

Further information is described in the module ORP.3 *Awareness and Training*.

IND.1.A3 Protection Against Malware

In order to prevent risks caused by malware, a concept for guarding against malware **MUST** be drawn up and implemented. In this concept, the threatened IT systems and the possible paths of infection (external interfaces, removable media, service and parametrising/programming devices) **MUST** be taken into account and suitable technical and organisational safeguards defined.

When using anti-virus software on OT components, it **MUST** be taken into consideration whether and in which configuration the operation of anti-virus software is supported by the manufacturer. If this is not the case, the need for alternative protection methods **MUST** be checked as part of a risk analysis.

The anti-virus software used **MUST** be supplied with up-to-date signatures. The virus protection concept **MUST** define the updating strategy. This includes the obtaining of signatures, their distribution procedures and the frequency of updates. The signatures can be obtained and distributed in an automated manner. The virus signatures **MUST NOT** be obtained by the OT systems directly from the Internet; they **MUST** be obtained indirectly via a proxy or virus sig-

nature distribution service. The interface systems **MUST** be operated in an independent zone (e.g. DMZ) that is separate from the OT environment.

Standard Requirements

For module IND.1 Operational and Control Technology, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

IND.1.A4 Documentation of the OT Infrastructure

The security-relevant parameters of the OT infrastructure **SHOULD** be documented. All software and system components **SHOULD** be documented in an inventory list. This list **SHOULD** state the product and protocol versions used, as well as the respective responsibilities. For the components used, possible restrictions of the manufacturers or regulatory conditions (such as certifications) **SHOULD** be defined. This documentation and a system inventory **SHOULD** be maintained – for example, in a control system.

In addition to this, an up-to-date network plan **SHOULD** document zones, zone transitions (conduits), and the communication protocols and methods used, as well as the external interfaces. For the interfaces, active network components and manual data transfer methods (e.g. using removable media) **SHOULD** be taken into account. The documentation **SHOULD** include redundancies, IP addresses or ranges and the assignment to physical security zones.

Since the documentation contains confidential information, all documents **MUST** be stored securely and classified with respect to their protection needs.

IND.1.A5 Development of a Suitable Zone Concept [IT Operation Department]

There **SHOULD** be a zone concept which defines different levels with different protection needs and includes the entire OT infrastructure, as well as the transition to office IT (at minimum). The network **SHOULD** be segmented according to the zones and the flow of data between the zones controlled in a suitable manner that makes attacks more complicated, less likely and more easily detectable.

There **SHOULD** also be horizontal segmentation in independent functional areas (such as systems). The individual zones **SHOULD** be as independent of one another as possible during operations. In particular, it **SHOULD** be possible to continue operating the zones in which the technical process is controlled for a predetermined period of time in the event of a failure of the other zones or their deliberate decoupling after being compromised. This period of time **SHOULD** be defined and documented as part of the risk analysis or, alternatively, as part of contingency planning. The network **SHOULD** therefore be designed so that it is stable, which means resistant to manipulations and errors.

All interfaces/connections between the zones **SHOULD** be subjected to a risk assessment. At the external interfaces, authenticated users and protocols with integrity protection **SHOULD** be used.

IND.1.A6 Change Management in OT Operations

For changes to the OT, a change process (change management) **SHOULD** be defined, documented and followed. The change process **SHOULD** ensure that changes are planned, documented, adequately tested for undesired side effects and functionality, objectively assessed with respect to security-relevant or operational effects and approved.

There SHOULD be a concept for the secure testing of changes. The system time of the OT infrastructure SHOULD be kept synchronous. This SHOULD be performed with an external reference.

Further information is described in the module OPS.1.2.1 *Change Management*.

IND.1.A7 Establishing Authorisation Management

The organisation SHOULD establish a process to manage user access and authorisations assigned for access to OT. The authorisation management SHOULD include the process, the implementation and documentation for the application, configuration and withdrawal of authorisations.

The authorisation management SHOULD ensure that authorisations are granted according to the minimum principle and checked at regular intervals. In the authorisation management, access to IT systems SHOULD be regulated for employees, administrators and third parties. Every party involved SHOULD receive regular training regarding the regulations to be fulfilled. Compliance SHOULD be checked and incorrect behaviour sanctioned.

Further information is described in module ORP.4 *Identity and Access Management*.

IND.1.A8 Secure Administration [IT Operation Department]

For initial configurations, management (administration) and remote maintenance in OT, either secure protocols or separate administration networks with corresponding protection needs SHOULD be used. Access to these interfaces SHOULD be restricted to the persons authorised. The access granted to systems and functions SHOULD be limited to that which is required for the respective administration task.

The systems and communication channels with which the administration or remote maintenance is performed SHOULD have the same level of protection as the OT components managed. Any remote maintenance and monitoring SHOULD be authorised, monitored and controlled by the organisation. For this purpose, the remote maintenance access SHOULD only be activated for use and deactivated again afterwards. This SHOULD be documented.

It SHOULD be taken into account that it is not possible to set up undesired tunnels in order to bypass security safeguards. In the case of higher protection needs, a dual control principle SHOULD also apply to critical administrative steps.

IND.1.A9 Restrictive Use of Removable Media and Mobile End Devices

Rules for the handling of removable media and mobile end devices SHOULD be established and communicated. As a matter of principle, the use of removable media and mobile end devices in ICS environments SHOULD be restricted. For the media and devices of service providers, an approval process and a requirements list SHOULD be available. Each service provider SHOULD be familiar with the specifications and confirm them in writing.

On the OT components, all interfaces which are not required SHOULD be deactivated. At the active interfaces, usage can be restricted to certain devices and media.

Further information is described in module SYS.3.4 *Mobile Storage Media*.

IND.1.A10 Monitoring, Logging and Detection [Area Security Officer]

To limit the possible effects of security incidents, relevant operational and security events SHOULD be identified in a timely manner. For this purpose, a suitable approach to log and event management SHOULD be developed and implemented. The log and event management SHOULD include adequate safeguards to ascertain and identify security-relevant events, as well as a response plan (security incident response).

The response plan SHOULD define procedures for the handling of security incidents. This plan SHOULD cover the classification of events, reporting channels and the definition of the organisational units to be involved, response plans to limit damage, the analysis and restoration of systems and services as well as the documentation of and follow-up process for incidents. The response plan SHOULD be tested and checked on a regular basis as whether it is up to date.

IND.1.A11 Secure Procurement and System Development

For the procurement, planning or development of ICS, regulations regarding information security SHOULD be drawn up and documented. The documents SHOULD be part of the tender.

During procurement, planning or development, information security SHOULD be taken into consideration through the entire lifecycle. Prerequisites and Implementation Guidance for the secure operation of OT components by manufacturers or integrators SHOULD be planned and implemented at an early stage. Compliance and implementation SHOULD be documented.

The organisation SHOULD document how the system integrates into the concepts for zoning, authorisation, vulnerability management and virus protection and adjust them if necessary. It SHOULD be regulated how operations can be maintained if one of the partners no longer provides services.

Further information is described in the module OPS.2.1 *Outsourcing for Customers*.

IND.1.A12 Establishing Vulnerability Management

For the secure operation of an ICS environment, the organisation SHOULD establish an approach to vulnerability management. The vulnerability management SHOULD identify gaps in software, components, protocols and external interfaces of the environment and derive, assess and implement possible requirements and opportunities for action (e.g. patch management).

The basis for this SHOULD be vulnerability messages (advisories) from manufacturers or publicly available CERT messages. In addition, organisational and technical audits can be performed for vulnerability analysis.

Requirements in Case of Increased Protection Needs

Generic suggestions for module IND.1 Operational and Control Technology are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

IND.1.A13 Contingency Planning for OT (A)

In cases where high availability is required, business continuity plans for situations in which each zone fails or is compromised SHOULD be defined, documented, tested after every major change and regularly drilled (see also BSI-Standard 100-4).

Moreover, an effective alternative procedure for cases in which the (remote) administration option fails SHOULD be defined, documented and tested.

IND.1.A14 Strong Authentication for OT Components (CIA)

For the secure authentication of privileged users in control systems, a central directory service SHOULD be set up. Authentication SHOULD be secured further using several factors (knowledge, ownership, biometrics).

During planning, it SHOULD be ensured that resulting dependencies in user authentication are known and taken into consideration when implementing the solution.

The central directory service SHOULD NOT be used for the authentication of operationally necessary technical accounts. When using a directory service, local system and application IDs for emergency situations SHOULD be set up and securely stored.

Authentication systems which manage sensitive authentication data SHOULD be adequately secured against unauthorised access, and changes SHOULD be documented in a transparent manner and monitored for abnormalities.

IND.1.A15 Verification and Monitoring of Authorisations (CIA)

In order to facilitate the effective verification of authorisations, the organisation SHOULD maintain an inventory list which includes all site access, system access, and data access rights that have been granted to critical systems. On the one hand, the list SHOULD provide information as to which rights a certain user effectively has, and, on the other, who has what rights to a certain system.

All critical administrative activities SHOULD be logged. The IT Operation Department SHOULD NOT be able to delete or manipulate the logs.

IND.1.A16 Stronger Compartmentalisation of Zones (IA)

In the case of ICS environments that have high protection needs or are difficult to secure at the system and network level, interface systems with security verification functions SHOULD be used to prevent risks arising from external connections.

As required in IND.1.A5 *Development of a Suitable Zone Concept*, all external interfaces of the environment SHOULD be subjected to a risk assessment. From the risks determined in the process, specific individual safeguards SHOULD be derived.

By realising one or several connection zones (DMZ) in a P-A-P structure (application layer gateways encapsulated by firewalls), continuous external connections CAN be terminated and necessary security checks (virus protection, formatting of data, checking and filtering of contents, media disruptions) performed without having to adjust the ICS system.

Implementing this requirement will increase perimeter security. Supplemental organisational and technical safeguards SHOULD be identified and implemented to further reduce risks that

arise from bypassing the perimeter deliberately or accidentally (using removable media or mobile devices, for example).

IND.1.A17 Regular Security Checks (I)

The security configuration of OT components SHOULD be checked at appropriate intervals or as needed in the case of sudden threats which were previously unknown. The security check SHOULD at least cover the exposed systems that feature external interfaces or user interaction. The realised security concept SHOULD also be checked at regular intervals. The security check SHOULD be carried out as a configuration check or also through automated conformity evaluations.

Additional Information

For more information about threats and security safeguards for module IND.1 *Operational and Control Technology*, see the following publications, among others:

[27019]	ISO/IEC 27019:2017: Information technology - Security techniques - Information security controls for the energy utility industry, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC, October 2017
[AHWAST]	White Paper, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme [Requirements for safe control and telecommunication systems]: German Association of Energy and Water Industries (BDEW) and Oesterreichs E-Wirtschaft, Version 2, May 2018, https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf , last accessed on 05.10.2018
[CSE]	Recommendations for further education and qualification measures in the ICS environment: BSI publications on cyber security (BSI-CS 123), November 2015, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_123.pdf , last accessed on 05.10.2018
[GART1]	Gartner IT Glossary: Operational Technology (OT), http://www.gartner.com/it-glossary/operational-technology-ot/ , last accessed on 05.10.2018
[ICSSK]	ICS Security Compendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten [Test recommendations and requirements for component manufacturers], Federal Office for Information Security (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html , last accessed on 05.10.2018
[ICSSKfH]	ICS Security Compendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten [Test recommendations and requirements for component manufacturers], Federal Office for Information Security (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html , last accessed on 05.10.2018
[IEC62443-2.1]	IEC 62443-2-1:2010 Industrial communication networks - Network and system security: Part 2-1: Establishing an industrial automation and control system security program, International Electrotechnical Commission (IEC), 2010, https://webstore.iec.ch/

	publication/7030 , last accessed on 05.10.2018
[WAST]	White Paper, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme [Requirements for safe control and telecommunication systems]: German Association of Energy and Water Industries (BDEW) Version 2.0, May 2018, https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/ , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module IND.1 *Operational and Control Technology*:

G 0.5 Natural Disasters

G 0.6 Catastrophes in the Vicinity

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

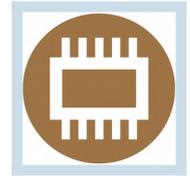
G 0.39 Malware

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0.5	G 0.6	G 0.9	G 0.11	G 0.14	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.23	G 0.28	G 0.29	G 0.30	G 0.32	G 0.36	G 0.37	G 0.39	G 0.41	G 0.42	G 0.46
IND.1.A1							X	X	X					X	X						
IND.1.A2		X			X			X								X		X		X	
IND.1.A3					X													X	X		
IND.1.A4			X		X					X	X					X					
IND.1.A5			X	X		X	X														
IND.1.A6			X	X	X												X				
IND.1.A7															X	X	X				
IND.1.A8				X	X			X		X	X			X							
IND.1.A9								X										X	X		X
IND.1.A10															X		X	X	X		
IND.1.A11							X		X		X	X									
IND.1.A12											X	X						X	X		
IND.1.A13	X	X	X	X																X	
IND.1.A14															X	X	X				
IND.1.A15															X	X	X				
IND.1.A16											X				X					X	
IND.1.A17														X	X	X					



IND.2.1: General ICS Components

Description

Introduction

An ICS component is an electronic component that controls or regulates a machine or system. It is thus part of an industrial control system (ICS) or, put more generally, operational technology (OT). Such components may include programmable logic controllers (PLC), sensors, actuators, a machine, or other parts of an ICS.

Due to the typically high availability requirements in the OT environment and the often extreme environmental conditions (climate, dust, vibration, corrosion), ICS components have always been designed to be robust devices with high reliability and long service life.

ICS components are normally configured and programmed using special software of the respective manufacturer. This is done using programming devices (e.g. as an application in Windows or Linux) or via an engineering station that loads the application programs into the programmable logic controllers.

The role of the Information Security Officer for the field of industrial automation has different names depending on the type and orientation of the organisation. Another name in addition to ICS Information Security Officer (ICS-ISO) is Industrial Security Officer.

Objective

The objective of this module is to secure any kinds of ICS components, regardless of manufacturer, type, purpose and application site. The module may be used for an individual device or for a modular device consisting of several components.

Not in Scope

The requirements have been drawn up for a generic component. For more specific ICS components, additional modules under IND.2 *ICS Components* describe requirements that go beyond the generic requirements of this module and may need to be implemented.

This module does not contain organisational requirements for safeguarding an ICS component. To this end, the requirements of module IND.1 *Operational and Control Technology* must be implemented.

Threat Landscape

For module IND.2.1 *General ICS Components*, the following specific threats and vulnerabilities are of particular importance:

Impairment Due to Harmful Environmental Influences

ICS components in industrial environments are often exposed to special conditions that can impair secure operations. Examples of this include extreme heat, cold, humidity, dust, vibration, or atmospheres with a corrosive or caustic effect. Frequently, several factors are present simultaneously. ICS components may wear more quickly and fail earlier due to such harmful environmental influences.

Incomplete Documentation

ICS components often are documented incompletely such that not all product features are known. In particular, the information about the services, protocols, communication ports and authorisation management are often incomplete. This makes the risk analysis more difficult because interfaces, functions and security-relevant mechanisms are overlooked. As a consequence, potential threats may not be taken into consideration. Moreover, it is only possible to a limited extent (or not at all) to react to new vulnerabilities of an ICS component if the services and ports used are not fully identified.

Insecure System Configuration

The default configuration of ICS components is mostly designed to ensure that the components work properly and can be commissioned easily. In this regard, security mechanisms often do not play a major role. This way, all services, protocols and connections are often activated and remain active in the default setting even if they are not used. Preset authorisations often remain unchanged, as well.

For attackers, it is easy to take over and manipulate such components. It is also possible for an attacker to exploit an insecure system configuration in order to use the ICS component as a starting point for additional attacks. As a result, business-critical information may be leaked or the entire operations of the organisation may be impaired.

Insufficient User and Authorisation Management

Some ICS components have their own user and authorisation management. If this is designed insufficiently, employees may make common use of user accounts, or the authorisations of employees who have left the company or service providers no longer working for the company may not be deleted. Overall, unauthorised persons may access ICS components this way.

Insufficient Logging

Regarding ICS components, logging is often limited to process-relevant events. Data relevant for information security is often not recorded. As a consequence, security incidents can only be detected with difficulty and cannot be reconstructed after the fact.

Manipulation and Sabotage of an ICS Component

The manifold interfaces of ICS components result in an increased risk of manipulations for systems, software and transmitted information. Depending on the motivation and knowledge

of the attacker, this may have effects locally or across multiple locations. Furthermore, status and alarm messages or other measured values may be suppressed or changed.

Manipulated measured values may cause ICS components or the operating personnel to make improper decisions. Manipulated systems may be used to attack other systems or locations or to cover up an ongoing manipulation.

Use of Insecure Protocols

Some of the protocols used within the framework of industrial control systems offer only limited security mechanisms (or none at all). Technical information such as measured and control values are often transmitted in plaintext and without integrity protection or authentication. An attacker with access to the transmission medium may, in this case, read out and modify the communication contents or implement control commands and thereby provoke actions or directly influence operations. An attack at the protocol level is possible even if the ICS component is configured securely otherwise and does not have any vulnerabilities.

Denial-of-Service (DoS) Attacks

An attacker may impair operations of ICS components with the help of DoS attacks. In the context of processes performed in real time, a short malfunction may already result in a loss of information or control.

Malware

The threat of malware is also becoming more and more serious in industrial control systems. Possible infections result from interfaces to the outside world and to office IT (vertical integration), but also from mobile devices such as service laptops or removable media when programming and maintaining ICS components. The latter can even install malware in isolated environments (overcoming the “air gap”).

Interception of Information / Espionage

ICS components frequently contain detailed information on the controlled or monitored process or procedure. This information may partially be reconstructed from other transmitted values such as measured or control data. The same holds true for control programs or parameters.

Attackers might obtain access to business secrets (industrial espionage), including recipes, processes or other intellectual property. They may also obtain information on the mode of operation of an ICS component and its security mechanisms that can be used for additional attacks.

Insufficient Security Requirements in Procurement

Information security is often not considered during procurement due to a lack of awareness of risks or for reasons of costs. As a consequence, serious vulnerabilities may sometimes be included in ICS components that may only be eliminated with great effort at a later point in time.

Manipulated Firmware

In addition to the application programs, the operating system (firmware) of ICS components may be changed. As a consequence, manipulated software may enter the system. Internal memory may be changed by an attacker by means of a compromised programming device, via

a local data interface (e.g. USB) or via another existing network connection. A software update might also have been manipulated along its way from the manufacturer to the operator. Ultimately, the operator might receive a component whose firmware has already been compromised – for example, in the event of a manipulated supply chain or when procuring from insecure sources. As a consequence, an attacker may modify or falsify processes and procedures.

Requirements

The specific requirements of module IND.2.1 *General ICS Components* are listed below. As a matter of principle, the ICS Information Security Officer is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	ICS Information Security Officer
Further Roles	ICS Administrator, Maintenance Personnel, Control Centre Operator

Basic Requirements

For module IND.2.1 *General ICS Components*, the following requirements **MUST** be implemented as a matter of priority:

IND.2.1.A1 Restricted Access to Configuration and Maintenance Interfaces [ICS Administrator]

It **MUST** be ensured that only authorised employees are allowed to access configuration and maintenance interfaces of ICS components. The configuration of the ICS component **MUST ONLY** be changed after an approval or authentication.

Default passwords configured and set by the manufacturer **MUST** be changed. The change **MUST** be documented and the password must be stored securely. Default user accounts configured and set by the manufacturer **SHOULD** be changed.

IND.2.1.A2 Use of Secure Protocols for Configuration and Maintenance [ICS Administrator, Maintenance Personnel]

Secure protocols **MUST** be used for configuring and maintaining ICS components. The data **MUST NOT** be transferred in an unprotected form.

IND.2.1.A3 Logging [ICS Administrator]

The following **MUST** be specified:

- which data/events is/are to be logged
- how long the logged data is to be stored
- who may view the data

In general, all security-relevant system events **MUST** be logged and analysed if required.

IND.2.1.A4 Disabling Unused Services, Features and Interfaces [Maintenance Personnel, ICS Administrator]

All services, features and interfaces of the ICS components that are not being used **MUST** be disabled or uninstalled.

IND.2.1.A5 Deactivating Unused User Accounts [ICS Administrator]

Unused or unnecessary user accounts **MUST** be deactivated.

IND.2.1.A6 Network Segmentation [ICS Administrator]

ICS components **MUST** be separated from the office IT. If ICS components depend on other components in the network, this **SHOULD** be documented sufficiently. ICS components **SHOULD** communicate as little as possible with other ICS components.

Standard Requirements

For module IND.2.1 *General ICS Components*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

IND.2.1.A7 Backups [Control Centre Operator]

Program and data backups **MUST** be generated regularly and after system changes.

IND.2.1.A8 Protection Against Malware [ICS Administrator]

ICS components **SHOULD** be protected against malware by suitable mechanisms. If an anti-virus protection program is used in this regard, the program and the virus signatures **SHOULD** always be up to date. If the resources on the ICS component are not sufficient or if the real-time requirement may be endangered by the use of anti-virus protection programs, alternative safeguards (such as the isolation of the component or the production network) **SHOULD** be implemented.

IND.2.1.A9 Documentation of Communication Relationships [ICS Administrator]

The systems with which an ICS component exchanges data and the data exchanged in this regard **SHOULD** be documented. Furthermore, the communication links of newly integrated ICS components **SHOULD** be documented.

IND.2.1.A10 System Documentation [Control Centre Operator, ICS Administrator]

Advanced system documentation **SHOULD** be drawn up. Particularities regarding operations (e.g. backups, regular maintenance measures, replacement and recovery of components, services of third parties) and the system administration options (e.g. remote access) **SHOULD** be documented therein. In addition, any changes to ICS components **SHOULD** be documented. It **SHOULD** be ensured that only authorised employees are allowed to access the system documentation. The documentation **SHOULD** be available in the event of incidents, as well.

IND.2.1.A11 Maintenance of ICS Components [Control Centre Operator, Maintenance Personnel, ICS Administrator]

The latest approved security updates **SHOULD** always be installed when maintaining an ICS component. Updates for the operating system **SHOULD** only be installed upon approval by the

manufacturer of the component, or the update SHOULD be tested in a test environment prior to being used in a production component. Maintenance SHOULD be performed on short notice for critical security updates.

IND.2.1.A12 Procurement of ICS Components [Control Centre Operator, ICS Administrator]

Uniform requirements for information security that correspond to the protection needs at hand SHOULD be defined for ICS components. These SHOULD be taken into consideration when procuring new ICS components.

IND.2.1.A13 Appropriate Commissioning of ICS Components [ICS Administrator]

Before they are commissioned, ICS components SHOULD correspond to the latest internally approved firmware, software and patch status.

New ICS components SHOULD be integrated into the existing operating, monitoring and information security management processes. This SHOULD include

- change and authorisation management
- vulnerability management
- protection against malware
- operational monitoring and contingency planning
- regular security checks on the systems

in particular.

IND.2.1.A14 Disposal of ICS components [ICS Administrator]

When disposing of legacy or defective ICS components, all sensitive data SHOULD be deleted securely. In particular, it SHOULD be ensured that all access data has been permanently removed.

IND.2.1.A15 Central System Logging and Monitoring [ICS Administrator]

All ICS components SHOULD transmit their logging data to a central system. The logged data SHOULD be evaluated regularly. In the event of security-critical events, automatic alarming SHOULD take place.

IND.2.1.A16 Protection of External Interfaces [ICS Administrator]

Interfaces accessible from the outside (e.g. network interfaces, USB ports or serial ports) SHOULD be protected against misuse.

IND.2.1.A17 Use of Secure Protocols for Transmitting Information [ICS Administrator]

Measured or control data SHOULD be protected against unauthorised access or changes. Regarding applications with real-time requirements, it SHOULD be checked whether this is necessary and feasible. If measured or control data is transmitted using public networks, it SHOULD be protected appropriately.

Requirements in Case of Increased Protection Needs

Generic suggestions for module IND.2.1 *General ICS Components* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

IND.2.1.A18 Communication During a Malfunction [Control Centre Operator, ICS Administrator]

There SHOULD be alternative and independent communication options that may be used in the event of malfunctions in order to maintain the ability to act.

IND.2.1.A19 Security Tests [ICS Administrator] (CIA)

With the help of regular security tests, it SHOULD be checked whether the technical security safeguards are still implemented efficiently. The security tests SHOULD NOT be carried out while the system is running. The tests SHOULD be scheduled for the maintenance periods. The results SHOULD be documented. Identified risks SHOULD be evaluated and addressed.

IND.2.1.A20 Trustworthy Code [ICS Administrator] (IA)

Firmware updates or new control programs SHOULD only be installed after their integrity and authenticity have been checked.

Additional Information

For more information about threats and security safeguards for module IND.2.1 *General ICS Components*, see the following publications, among others:

[AHWAST]	White Paper, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme [Requirements for safe control and telecommunication systems]: German Association of Energy and Water Industries (BDEW) and Oesterreichs E-Wirtschaft, Version 2, May 2018, https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf , last accessed on 05.10.2018
[ICSSK]	ICS Security Compendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten [Test recommendations and requirements for component manufacturers], Federal Office for Information Security (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html , last accessed on 05.10.2018
[ICSSkfH]	ICS Security Compendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten [Test recommendations and requirements for component manufacturers], Federal Office for Information Security (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html , last accessed on 05.10.2018
[NIST80082]	Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-81, Revision 2, September 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf , last accessed on 05.10.2018

[WAST]	White Paper, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme [Requirements for safe control and telecommunication systems]: German Association of Energy and Water Industries (BDEW) Version 2.0, May 2018, https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/ , last accessed on 05.10.2018
--------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module IND.2.1 *General ICS Components*:

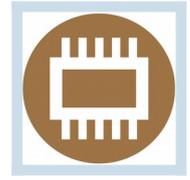
- G 0.2 Unfavourable Climatic Conditions
- G 0.4 Pollution, Dust, Corrosion
- G 0.8 Failure or Disruption of the Power Supply
- G 0.9 Failure or Disruption of Communication Networks
- G 0.10 Failure or Disruption of Supply Networks
- G 0.12 Electromagnetic Interference
- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.19 Disclosure of Sensitive Information
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.28 Software Vulnerabilities or Errors
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.37 Repudiation of Actions
- G 0.39 Malware
- G 0.40 Denial of Service
- G 0.41 Sabotage

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0. 2	G 0. 4	G 0. 8	G 0. 9	G 0. 10	G 0. 12	G 0. 14	G 0. 15	G 0. 19	G 0. 21	G 0. 22	G 0. 23	G 0. 25	G 0. 28	G 0. 30	G 0. 31	G 0. 32	G 0. 37	G 0. 39	G 0. 40	G 0. 41	G 0. 43	G 0. 45	G 0. 46
IND.2.1. A1							X		X	X		X			X	X					X	X	X	X
IND.2.1. A2							X		X	X		X						X			X			X
IND.2.1. A3									X	X						X	X				X	X		
IND.2.1. A4							X	X	X	X	X	X			X						X			
IND.2.1. A5							X	X	X	X	X	X			X						X			
IND.2.1. A6							X	X		X	X	X			X	X	X		X	X	X			
IND.2.1. A7	X	X	X	X	X	X							X						X	X	X			X
IND.2.1. A8							X		X	X	X	X	X	X	X				X					
IND.2.1. A9				X			X	X			X							X			X			X
IND.2.1. A10							X		X	X				X	X				X		X	X	X	X
IND.2.1. A11							X		X	X		X		X	X	X	X		X		X			
IND.2.1. A12	X	X				X		X		X			X	X					X					
IND.2.1. A13						X	X	X		X		X	X	X					X		X			



IND.2.2: Programmable Logic Controller (PLC)

Description

Introduction

A programmable logic controller (PLC) is an ICS component. It performs control tasks of operational technology (OT). The boundaries between different device classes and designs are fluid today. For example, a remote terminal unit (RTU) may take over the functions of a PLC, or a programmable automation controller (PAC) may try to combine the benefits of a PLC and an industrial PC. However, the PLC is still the classic automation device, which is why these terms are used synonymously in this module.

A PLC has digital inputs and outputs, a real-time operating system (firmware) and further interfaces for Ethernet or fieldbuses. The connection to sensors and actuators is made via the analogue or digital inputs and outputs, or via a fieldbus. Communication with the process control system typically takes place via the Ethernet interface and IP-based networks.

The possible realisations are manifold: a programmable logic controller can be used as an assembly, a single device, a PC plug-in card (slot PLC) or as software emulation (soft PLC). Modular programmable logic controllers composed of various functional plug-in modules are the most frequent type. Further functions like visualisation, alerting and logging are also performed increasingly by the PLC.

Due to the typically high availability requirements in the OT environment and the often extreme environmental conditions (climate, dust, vibration, corrosion), ICS components have always been designed to be robust devices with high reliability and long service life.

A PLC is normally configured and programmed using special software of the respective manufacturer. This is performed either by programming devices (e.g. as an application in Windows or Linux) or by an engineering station that distributes the data via a network.

Objective

The aim of this module is to protect any type of programmable logic controllers irrespective of manufacturer, type, purpose and place of use. It can be used for an individual PLC or for a combined assembly used as a PLC.

Not in Scope

The present system module is to be used for protecting all types of programmable logic controllers (i.e. a PLC and devices that integrate identical or similar functions). It supplements module IND.2.1 *General ICS Components*. This should also be considered during application.

This module does not contain organisational requirements for safeguarding an ICS component. To this end, the requirements of module IND.1 *Operational and Control Technology* must be implemented. The area of functional safety is also not addressed.

Threat Landscape

For module IND.2.2 *Programmable Logic Controller (PLC)*, the following specific threats and vulnerabilities are of particular importance:

Incomplete Documentation

Programmable logic controllers are often documented incompletely so that not all product functions are known. In particular, the information about the services, protocols, communication ports and authorisation management are often incomplete. However, this complicates analysis of threats as interfaces, functions and security-relevant mechanisms can be overlooked. As a consequence, potential threats may not be taken into consideration. Furthermore, if new vulnerabilities are not recorded, the response to them may be limited, if not impossible.

Requirements

The specific requirements of module IND.2.2 *Programmable Logic Controller (PLC)* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	ICS Information Security Officer
Further Roles	ICS Administrator

Basic Requirements

For module IND.2.2 *Programmable Logic Controller (PLC)* there are no Basic Requirements

Standard Requirements

For module IND.2.2 *Programmable Logic Controller (PLC)*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

IND.2.2.A1 Extended System Documentation for Programmable Logic Controllers [ICS Administrator]

If control programs and configurations are changed, they SHOULD always be archived. Changes in configurations and the replacement of components SHOULD be documented completely.

IND.2.2.A2 User Account Control and Restrictive Assignment of Rights [ICS Administrator]

Access rights to functions and interfaces of an PLC SHOULD be granted restrictively. It SHOULD be checked regularly whether existing user accounts are still required and the assigned authorisations are still correct. If the responsibilities of the employees change, the authorisations SHOULD be updated promptly.

IND.2.2.A3 Time Synchronisation [ICS Administrator]

Centrally automated time synchronisation SHOULD be established for the system time.

Requirements in Case of Increased Protection Needs

For module IND.2.2 *Programmable Logic Controller (PLC)* there are no Requirements in Case of Increased Protection Needs

Additional Information

Currently there is no additional information on threats and security measures for module IND.2.2 *Programmable Logic Controller (PLC)*.

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module IND.2.2 *Programmable Logic Controller (PLC)*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.19 Disclosure of Sensitive Information

G 0.21 Manipulation with Hardware or Software

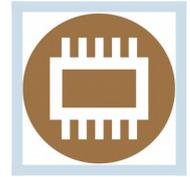
G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.41 Sabotage

Elementary Threats Requirements	G 0.14	G 0.15	G 0.19	G 0.21	G 0.22	G 0.23	G 0.30	G 0.41
IND.2.2.A1				X	X	X		X
IND.2.2.A2	X	X	X	X	X	X	X	X
IND.2.2.A3				X	X			



IND.2.3: Sensors and Actuators

Description

Introduction

As electronic components featuring a microprocessor and software, sensors are measuring transducers that convert a physical magnitude into an electrical output value. This value is provided as a standardised unit signal (often 4 to 20mA, 0 to 10V) to a serial interface, or as digital information transmitted via a fieldbus or Ethernet protocols. In addition to the measurement values, measuring transducers often provide interfaces for performing diagnosis and parametrisation. In addition to an electronic output value, a sensor may have further interfaces (e.g. WLAN, Bluetooth or wireless HART interfaces) for parametrisation and diagnosis.

There are many different sensors available on the market, including for measuring physical magnitudes. Depending on the task, the functions and the performance of a sensor vary significantly. The spectrum includes sensors that only provide measurement values and do not require configuration; sensors that enable calibration, configuration or pre-processing of data; and complete signal processing (intelligent sensors, smart sensors).

Objective

The aim of this module is to protect any type of smart sensor irrespective of manufacturer, type, purpose and place of use. It can be used for an individual sensor or for a combined assembly used as a sensor.

Not in Scope

The present system module is to be used to protect smart sensors. It supplements the generic module IND.2.1 *General ICS Components*, which is a prerequisite of the present module.

The module does not address simple sensors with configuration interfaces or more complex processing logic, as in such cases the possible security safeguards are limited to protecting the sensor and monitoring it to detect whether it is active.

The module does not address the protection of complex wireless sensor networks either. It only describes the protection of individual sensors. Security requirements for operational and control technology are also not described. Here, module IND.1 *Operational and Control Technology* must be implemented.

Threat Landscape

For module IND.2.3 *Sensors and Actuators*, the following specific threats and vulnerabilities are of particular importance:

Insufficient Security Requirements in Procurement

Information security is often not considered during procurement due to a lack of awareness of risks or for reasons of costs. Sensors might thus include serious vulnerabilities that can be removed only with significant effort later on.

Sensors for ICS components in industrial environments are frequently subject to particular conditions that affect their secure operation. Examples of this include extreme heat, cold, humidity, dust, vibration, or atmospheres with a corrosive or caustic effect. Frequently, several factors are present simultaneously. Such harmful environmental impacts may result in the sensors of ICS components wearing more rapidly, failing earlier or measuring incorrect values.

Requirements

The specific requirements of module IND.2.3 *Sensors and Actuators* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	ICS Information Security Officer
Further Roles	ICS Administrator, Maintenance Personnel

Basic Requirements

For module IND.2.3 *Sensors and Actuators*, the following requirements **MUST** be implemented as a matter of priority:

IND.2.3.A1 Installation of Sensors [Maintenance Personnel, ICS Administrator]

Sensors **MUST** be installed in a suitable manner. The sensors **MUST** be sufficiently robust and reliable to be able to perform measurements under the intended environmental conditions (in terms of climate, dust, vibration, corrosion, etc).

Standard Requirements

For module IND.2.3 *Sensors and Actuators*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

IND.2.3.A2 Calibration of Sensors [Maintenance Personnel]

If necessary, sensors **SHOULD** be calibrated regularly. Calibrations **SHOULD** be documented appropriately. Access to calibration **MUST** be protected because the intentional mis-calibration of a sensor may result in an attack vector.

Requirement in Case of Increased Protection Needs

Generic suggestions for module IND.2.3 *Sensors and Actuators* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

IND.2.3.A3 Wireless Communication (C)

In case of increased protection needs, wireless management interfaces such as Bluetooth, WLAN or NFC SHOULD NOT be used. Any unused communication interfaces MUST be disabled.

Additional Information

Currently there is no additional information on threats and security measures for module IND.2.3 *Sensors and Actuators*.

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module IND.2.3 *Sensors and Actuators*:

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

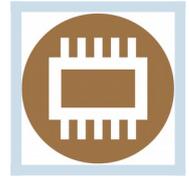
G 0.21 Manipulation with Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

Elementary Threats Requirements	G 0.14	G 0.18	G 0.21	G 0.23	G 0.28	G 0.30
IND.2.3.A1	X	X				X
IND.2.3.A2	X		X		X	X
IND.2.3.A3	X	X	X	X	X	X



IND.2.4: Machine

Description

Introduction

A machine is a technical device that performs automated tasks. A typical example would involve a machine-tool that processes products in a pre-defined manner. It is controlled by an IT system using a program that provides the corresponding work instructions and steps. Such machines are also referred to as automatons.

In most cases, machines are designed by mechanical engineers and provided with pre-defined functions. However, the operator of the machine may define the parameters used by the machine for working. Shapes to be milled or calibrations for certain materials can thus be set. Machines have various interfaces (e.g. for removable data media, specialised programming devices or network access) so that the operator can change the parameters.

Frequently, mechanical engineers also offer remote maintenance services for early detection of wear or the ability to respond quickly in case of problems.

Objective

This module describes how electronically controlled, semi-automatic or fully automatic machines (e.g. CNC machines) can be protected irrespective of manufacturer, type, special purpose and place of use.

Not in Scope

The present module supplements the generic module IND.2.1 *General ICS Components* and requires its prior implementation. Furthermore, it only defines requirements for machines whose internal structures cannot be accessed by an organisation.

Security requirements for operational and control technology are not described either. Module IND.1 *Operational and Control Technology* must be implemented in this regard. The area of functional safety is also not addressed.

Threat Landscape

For module IND.2.4 *Machine*, the following specific threats and vulnerabilities are of particular importance:

Failure or Disruption Due to Insufficient Maintenance

If machines are not maintained regularly, they will not work correctly at an earlier point in time or will fail completely. Malfunctions may threaten employees, for example, or significantly impair production.

Targeted Manipulations

If the interfaces of a machine are protected insufficiently, attackers may manipulate the parameters of the machine (e.g. via local programming devices or network services). This may damage workpieces or result in entire product series that are defective. However, the attackers may also damage the machine itself, resulting in an economic loss, as well.

Requirements

The specific requirements of module IND.2.4 *Machine* are listed below. As a matter of principle, the ICS Information Security Officer (ICS-ISO) is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	ICS Information Security Officer
Further Roles	ICS Administrator

Basic Requirements

For module IND.2.4 *Machine*, the following requirements **MUST** be implemented as a matter of priority:

IND.2.4.A1 Remote Maintenance by Mechanical and System Engineers [ICS Administrator]

There **SHOULD** be a central policy for remote maintenance of a machine. This **SHOULD** regulate how the corresponding remote maintenance solutions are to be used and how communication links are protected. It **SHOULD** also describe the activities to be monitored during remote maintenance.

Moreover, it **SHOULD NOT** be possible to access other systems or machines of the organisation via remote maintenance of a machine.

The manner in which the information stored in the machine is to be processed **SHOULD** be agreed with a service provider.

IND.2.4.A2 Operation After End of Warranty [ICS Administrator]

A process designed to ensure that the machine can be securely operated beyond the warranty period **SHOULD** be established. To this end, further support services **SHOULD** be contractually agreed with the supplier.

Standard Requirements

For module IND.2.4 *Machine* there are no *Standard Requirements*

Requirements in Case of Increased Protection Needs

For the module IND.2.4 *Machine* there are no Requirements in Case of Increased Protection Needs.

Additional Information

Currently there is no additional information on threats and security measures for module IND.2.4 *Machine*.

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module IND.2.4 *Machine*:

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

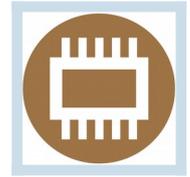
G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.39 Malware

Elementary Threats Requirements	G 0.11	G 0.14	G 0.18	G 0.21	G 0.22	G 0.30	G 0.39
IND.2.4.A1	X	X	X	X	X	X	
IND.2.4.A2				X			X



IND.2.7: Safety Instrumented Systems

Description

Introduction

Safety instrumented systems (SIS) are a subgroup of industrial control systems (ICS). SIS are used to avert threats to technical installations, the environment and people. There is very little difference between the basic structure of an SIS and a conventional automation system. The main difference relates to the increased reliability requirements that apply to how the security functions (SIF) to be executed by an SIS are performed. The level of reliability is expressed by the four-level safety integrity level (SIL; see [IEC 61508]). SIL1 is the lowest reliability requirement, and SIL4 is the highest. Depending on the SIL level, different requirements then apply to the permissible failure rate of components, the hardware fault tolerance of the architecture, the independence of auditors and other points. The entire lifecycle of an SIS is organisationally embedded in a functional safety management (FSM) system.

This module must be implemented regardless of the SIL level at hand. Information security must be taken into account in every lifecycle phase, from the development of the components to their application, operation and decommissioning. Ensuring the integrity of the SIS has the highest priority in this regard.

Another key feature of an SIS is its independence and separation from surrounding IT systems and operational technology (OT). In other words, the availability and integrity of the SIS must not be influenced by these adjacent elements.

Objective

The objective of the module is to formulate appropriate SIS requirements that are to be met when establishing an information security management system (ISMS).

For the purposes of this module, the term “SIS” includes the sensor, the actuator, the safety-related programmable logic controller (PLC, also known as the logic system), the application program and, in particular, the associated programming devices (engineering station, hand-held devices for sensor-actuator configuration) and visualisation devices.

Not in Scope

This module supplements the generic modules IND.1 *Operational and Control Technology*, IND.2.1 *General ICS Components* and assumes that these modules have been observed.

Since standard IT systems are generally used as programming devices and visualisation equipment, the requirements from module SYS.2.1 *General Client* and the respective operating-system-specific client modules must be implemented in addition to the requirements in this module.

Threat Landscape

For module IND.2.7 *Safety Instrumented Systems*, the following specific threats and vulnerabilities are of particular importance:

Manipulation of the Logic System

The manipulation of the application program on the logic system, which can violate the integrity of a SIS, represents the greatest risk. Unlike with “simple” OT components, this can have potentially serious or extremely severe consequences on the security of people, the environment and technical installations. On worksheet NA 163 from the international User Association of Automation Technology in Process Industries (NAMUR) [NA 163], the following three categories are defined in this respect:

- Category 1 is a group of hazards that lead to manipulation of the logic system, whereby the security function (SIF) is triggered despite there being no corresponding need. The consequences are not dangerous in terms of functional security because the SIS will initiate its safe mode, but this does lead to a business interruption. This can be caused, for example, by malware or human error.
- Category 2 describes cases where the SIF is disabled, which means protection is no longer available. An unacceptable result is not achieved until a situation requiring action arises. The consequences are classified as dangerous because the SIS cannot fulfil its primary task. Attack scenarios are classified as complex because manipulation of the logic system alone is not sufficient to cause damage.
- The third category deals with the worst-case scenario, where one or more SIFs are deactivated and a situation requiring action is caused intentionally. This is another case in which the effects are classified as dangerous and the attack scenarios as very complex. In addition to knowledge of how to manipulate the SIS, the perpetrators must also have sound knowledge of the physical process in order to be able to cause a situation that requires action.

In December 2017, the first-ever reports were published on malware that had deliberately manipulated SIS. The perpetrators had gained entry via the engineering station, where the special software for programming and parameterisation was located. From there, the malware installed searched specifically for connected logic systems from a certain manufacturer and loaded executable code onto them, which manipulated the application program (the logic). The validity check failed due to an error in this code. As a result, the security function was triggered and the attacked system was put into safe mode. Although the attack was not successful, its impact and complexity could have been classified as Category 2 or 3 [Triton].

Inadequate Monitoring and Detection Procedures

An essential function of automation systems involves monitoring the operating states of the process to be automated. This usually includes warnings concerning the process (e.g. if fill levels are exceeded) and technical parameters (e.g. temperatures, valve positions). In contrast, the supporting IT infrastructure is often not monitored.

If unusual or security-relevant events are not or only inadequately monitored, attempted attacks, network bottlenecks or foreseeable failures cannot be detected at an early stage.

Requirements

The specific requirements of module IND.2.7 *Safety Instrumented Systems* are listed below. As a matter of principle, the Operations Manager is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Operations Manager
Further Roles	Planner, Maintenance Personnel, Manufacturer, ICS Information Security Officer

Basic Requirements

For module IND.2.7 *Safety Instrumented Systems*, the following requirements **MUST** be implemented as a matter of priority:

IND.2.7.A1 Recording and Documentation [Planner, Maintenance Personnel]

All hardware and software components belonging to the SIS, relevant information, connections, roles and responsibilities **MUST** be recorded and documented separately.

IND.2.7.A2 Specified Use of Hardware and Software Components [Maintenance Personnel]

The hardware and software components belonging to or used in connection with the SIS **MAY NOT** be used for any other purpose.

IND.2.7.A3 Changing the Application Program on the Logic System [Maintenance Personnel]

Existing protection mechanisms on the logic system **MUST** be activated. If this is not possible, alternative measures **MUST** be taken. User programs on the logic systems **MUST** only be changed or released for transmission by authorised persons.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module IND.2.7 *Safety Instrumented Systems*. They **SHOULD** be implemented as a matter of principle.

IND.2.7.A4 Anchoring Information Security in Functional Safety Management [ICS Information Security Officer]

All processes and responsibilities pertaining to the information security of SIS **SHOULD** be clearly defined. These **SHOULD** be described and named as part of functional safety management.

IND.2.7.A5 SIS Business Continuity Management [ICS Information Security Officer]

The manner in which security incidents are to be handled SHOULD be defined in an incident response plan. This plan SHOULD define the roles and responsibilities and include the measures to be taken.

IND.2.7.A6 Secure Planning and Specification of SIS [Planner, Maintenance Personnel, ICS Information Security Officer]

Accidental or unauthorised changes to the specification, implementation or engineering data SHOULD be prevented.

IND.2.7.A7 Separation and Independence of the SIS from the Environment [Planner, Maintenance Personnel]

The SIS SHOULD be independent of its environment in order to guarantee its security functions. Processes that have a potential impact on the SIS SHOULD be subject to the change management process established for functional safety management.

IND.2.7.A8 Secure Transfer of Engineering Data to SIS [Planner, Maintenance Personnel, ICS Information Security Officer]

The integrity of the engineering data SHOULD be ensured during transmission.

IND.2.7.A9 Protection of Data and Signal Connections [Planner, Maintenance Personnel, ICS Information Security Officer]

If it cannot be proven that data and signal connections are not subject to feedback effects (unidirectionality), these connections SHOULD be suitably protected.

IND.2.7.A10 Displays and Alerts Pertaining to Simulated or Bridged Variables [Planner]

SIS variables that are occupied (simulated) by substitute values or bridged externally SHOULD be monitored in an appropriate manner. The values SHOULD be displayed continuously to the operator. Limit values SHOULD be defined. If these limit values are reached, a suitable alert SHOULD be sent to those responsible.

IND.2.7.A11 Dealing with Integrated Systems [Planner, Maintenance Personnel, ICS Information Security Officer]

For integrated systems, a suitable strategy SHOULD be developed that defines how the safety-related aspects are to be handled.

Requirement in Case of Increased Protection Needs

Generic suggestions for module IND.2.7 *Safety Instrumented Systems* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

IND.2.7.A12 Ensuring the Integrity and Authenticity of Application Programs and Configuration Data [Planner, Manufacturer] (I)

Care SHOULD be taken to ensure that manufacturers develop and integrate appropriate mechanisms to ensure the integrity and authenticity of configuration data and application programs

on the logic system or associated sensors and actuators. Any software that is offered for download SHOULD be protected from manipulation. Integrity violations SHOULD be detected and reported automatically.

Additional Information

Interesting Facts

In terms of safety instrumented systems, all the necessary information is contained in this module, the Implementation Guidance and the literature overview.

References

For more information about threats and security safeguards for module IND.2.7 *Safety Instrumented Systems*, see the following publications, among others:

[27019]	ISO/IEC 27019:2017: Information technology - Security techniques - Information security controls for the energy utility industry, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC, October 2017
[AHWAST]	White Paper, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme [Requirements for safe control and telecommunication systems]: German Association of Energy and Water Industries (BDEW) and Oesterreichs E-Wirtschaft, Version 2, May 2018, https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf , last accessed on 05.10.2018
[ICSSK]	ICS Security Compendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten [Test recommendations and requirements for component manufacturers], Federal Office for Information Security (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html , last accessed on 05.10.2018
[ICSSKfH]	ICS Security Compendium: Testempfehlungen und Anforderungen für Hersteller von Komponenten [Test recommendations and requirements for component manufacturers], Federal Office for Information Security (BSI), November 2014 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/ICS/ICS-Security-Kompendium-Hersteller.html , last accessed on 05.10.2018
[IEC61508-1]	IEC 61508-1:2010 Functional safety of electrical/electronic/programmable electronic safety-related systems: Part 1: General requirements, International Electrotechnical Commission (IEC) https://webstore.iec.ch/publication/22273 , last accessed on 05.10.2018
[IEC61511]	IEC 61511-1:2016 Functional safety - Safety instrumented systems for the process industry sector: International Electrotechnical Commission (IEC) https://webstore.iec.ch/publication/5527 , last accessed on 05.10.2018
[IEC62443-2.1]	IEC 62443-2-1:2010 Industrial communication networks - Network and system security: Part 2-1: Establishing an industrial automation and control system security program, International Electrotechnical Commission (IEC), 2010, https://webstore.iec.ch/

	publication/7030 , last accessed on 05.10.2018
[IEC62443-2.4]	IEC 62443-2-4:2015: Security for industrial automation and control systems: Part 2-4: Security program requirements for IACS service providers, International Electrotechnical Commission (IEC) https://webstore.iec.ch/publication/22810 , last accessed on 05.10.2018
[IEC62443-4.1]	IEC 62443-4-1:DRAFT: Security for industrial automation and control systems - Technical security requirements for IACS components: Part 4-1: Secure product development life-cycle requirements, International Electrotechnical Commission (IEC)
[IEC62443-4.2]	IEC 62443-4-2:DRAFT: Technical security requirements for IACS components: Part 4-2: Technical security requirements for IACS components, International Electrotechnical Commission (IEC)
[NA163]	NA 163 Security Risk Assessment of SIS: International User Association of Automation Technology in Process Industries (NAMUR), NA 163 Security Risk Assessment of SIS, https://www.namur.net/ (last accessed on 11.04.2018; access is subject to a fee)
[NIST80082]	Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-81, Revision 2, September 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf , last accessed on 05.10.2018
[TRITON]	FireEye: Attackers Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html , last accessed on 05.10.2018
[VDE2180]	Safeguarding of industrial process plants by means of process control engineering (PCE): Technical Rule VDI/VDE 2180 Safeguarding of industrial process plants by means of process control engineering (PCE)
[VDE2182.2.3]	Technical Rule VDI/VDE 2182 Part 2.3 "IT-security for industrial automation - Example of use of the general model for operators in factory automation - Stamping plant"
[VDE2182.3.3]	Technical Rule VDI/VDE 2182 Part 3.3 "IT-security for industrial automation - Example of use of the general model for plant managers in process industry - LDPE-plant"
[VDI2182.1]	Technical Rule VDI/VDE 2182 Part 1, IT-security for industrial automation - General model, January 2011
[WAST]	White Paper, Anforderungen an sichere Steuerungs- und Telekommunikationssysteme [Requirements for safe control and telecommunication systems]: German Association of Energy and Water Industries (BDEW) Version 2.0, May 2018, https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/ , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module IND.2.7 *Safety Instrumented Systems*:

- G 0.5 Natural Disasters
- G 0.6 Catastrophes in the Vicinity
- G 0.9 Failure or Disruption of Communication Networks
- G 0.11 Failure or Disruption of Service Providers
- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.20 Information or Products from an Unreliable Source
- G 0.21 Manipulation with Hardware or Software
- G 0.23 Unauthorised Access to IT Systems
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.36 Identity Theft
- G 0.37 Repudiation of Actions
- G 0.39 Malware
- G 0.41 Sabotage
- G 0.42 Social Engineering
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0. 5	G 0. 6	G 0. 9	G 0. 11	G 0. 14	G 0. 15	G 0. 18	G 0. 19	G 0. 20	G 0. 21	G 0. 23	G 0. 28	G 0. 29	G 0. 30	G 0. 32	G 0. 36	G 0. 37	G 0. 39	G 0. 41	G 0. 42	G 0. 46
IND.2.7.A1					X	X		X		X	X			X					X	X	X
IND.2.7.A2					X	X		X		X	X			X					X	X	X
IND.2.7.A3										X									X	X	X
IND.2.7.A4	X	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	
IND.2.7.A5	X	X	X	X	X														X		
IND.2.7.A6	X	X	X	X	X	X	X	X	X	X	X								X		
IND.2.7.A7		X	X		X	X		X		X	X								X	X	X
IND.2.7.A8									X	X	X								X		X
IND.2.7.A9			X		X	X		X		X	X								X		X
IND.2.7.A10											X								X	X	
IND.2.7.A11		X			X	X		X	X	X	X								X	X	X
IND.2.7.A12									X	X	X	X							X		



NET.1.1: Network Architecture and Design

Description

Introduction

Today, most organisations require computer networks for their business operations – for example, for the exchange of data or the implementation of shared applications. In addition to conventional end devices, partner organisations and the Internet, these networks increasingly integrate mobile end devices and elements attributed to the Internet of Things (IoT). Moreover, cloud services and services for unified communications and collaboration (UCC) are increasingly being used via computer networks. The resulting benefits are undisputed. The large number of end devices and services, however, also increases the risks. It is therefore important that organisations protect their own networks with secure network architecture. To this end, it must be planned how a local area network (LAN) or a wide area network (WAN) can be built with a secure architecture. In addition, external networks that can only be trusted to a limited extent (e.g. the Internet or customer networks) must be integrated in a suitable manner.

To ensure a high level of security, additional security-relevant aspects have to be considered: for example, different clients and device groups should be securely separated on the network level and their communication should be controlled using firewall technologies. Another important security element, particularly in the client area, is network access control (see NET.1.3 *Network Access Control*).

Objective

The objective of this module is to establish information security as an integral component of network architecture and design.

Not in Scope

The module contains basic requirements which have to be considered and met when planning, designing and operating new networks. Requirements for the secure operation of the relevant network components, including security components such as firewalls and intrusion detection systems/intrusion prevention systems (IDS/IPS), are not discussed in the present module. They are addressed in the module group NET.3 *Network Components*.

The focus of this module is on cable-based networks and data communication. However, general requirements for architecture and design (e.g. separating security zones and segments) must be observed and met for all network technologies. Additional specific requirements for network areas such as wireless (WLAN) or storage area networks (SAN) are addressed in the module groups NET.2 *Radio Networks* and in module SYS.1.8 *Storage Solutions*. The subjects of

UCC and Voice over IP (VoIP), as well as the underlying security infrastructure, are also not discussed in this module; they are addressed in the corresponding modules NET.4.2 *VoIP* and NET.4.5 *Unified Communications*.

Specific security-related requirements for virtual private clouds and hybrid clouds are not the focus of this module (see OPS.3.2 *Cloud Providers* and OPS.3.4 *Managed Security Services*).

Network management is considered within the scope of zoning and segmentation, while all other subjects of network management are addressed in module NET.1.2 *Network Management*.

Threat Landscape

For module NET.1.1 *Network Architecture and Design*, the following specific threats and vulnerabilities are of particular importance:

Failure or Insufficient Performance of Communication Links

If the communication links have insufficient capacity or their performance is no longer sufficient as a consequence of technical failures or denial-of-service (DoS) attacks, the communication of clients with servers (for example) will be restricted. As a result, the access times for internal and external services (e.g. cloud services) will increase, and the use of these services may be restricted or no longer possible. It may also be the case that business-relevant information is no longer available. This can result in a loss of production or essential business processes.

Inadequately Secured Network Access

If the internal network is connected to the Internet and the transition is not sufficiently protected (e.g. due to lack of or incorrectly configured firewalls), attackers can access sensitive information of the organisation and copy or manipulate it.

Inadequate Network Structuring

If the structure or expansion of a network is inadequate, insecure network topologies and network configurations may arise. This allows attackers to easily identify vulnerabilities and penetrate the organisation's internal network, where they can retrieve information, manipulate data or disrupt entire production systems. In an incorrectly structured network, where monitoring by the security systems is limited, attackers also remain unnoticed for longer periods of time.

Requirements

The specific requirements of module NET.1.1 *Network Architecture and Design* are listed below. As a matter of principle, the Head of Networks is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	Head of Networks
---------------------	------------------

Further Roles	Chief Information Security Officer (CISO), IT Operation Department, Head of IT
----------------------	--------------------------------------------------------------------------------

Basic Requirements

For module NET.1.1 *Network Architecture and Design*, the following requirements **MUST** be implemented as a matter of priority:

NET.1.1.A1 Network Security Policy [Head of IT, Chief Information Security Officer (CISO)] (I)

Based on the organisation's general security policy, a specific security policy for the network **MUST** be developed which transparently describes requirements and specifications regarding the secure design and structuring of networks. The following, among other things, **MUST** be defined in this policy:

- the cases in which the security zones have to be segmented and user groups or clients have to be separated logically or even physically
- which communication relationships and which network and application protocols are permitted in each case
- how the data traffic for administration and monitoring is to be separated in the network
- which internal, cross-location communication (WAN, wireless networks) is allowed and which encryption is required on the WAN, LAN or radio links
- which cross-location communication is permitted

The policy **MUST** be known to all employees responsible in the area of network design and recognised as essential to their work. If the policy is changed or the requirements are not fully met, this **MUST** be documented and agreed with the CISO in charge. The correct implementation of the policy **MUST** be regularly reviewed. The results **MUST** be documented in an appropriate manner.

NET.1.1.A2 Documentation of the Network [IT Operation Department]

A complete documentation of the network (including a network plan) **MUST** be prepared and consistently maintained. This documentation **MUST** contain the initial survey of the actual situation (including network performance) and all changes made to the network. The logical structure of the network **MUST** also be documented, in particular the assignment of sub-networks and the zoning and segmentation of the network.

NET.1.1.A3 Specification of Network Requirements

Based on the security policy (see NET.1.1.A1 *Network Security Policy*), a specification of network requirements **MUST** be developed and consistently maintained. It **MUST** be possible to derive all main elements for the network architecture and design from these requirements.

NET.1.1.A4 Network Separation in Security Zones

The overall network **MUST** be physically separated into the following three security zones at minimum: internal network, demilitarised zone (DMZ) and external connections (including to the Internet and other untrusted networks). Transitions between the zones **MUST** be protected

by a firewall. This control **MUST** follow the principle of local communication so that firewalls forward only authorised communications (whitelisting).

Untrusted networks (e.g. the Internet) and trusted networks (e.g. an intranet) **MUST** be separated by a two-stage firewall structure consisting of stateful packet filters (firewall). In order to separate the Internet and external DMZ in the network, a stateful packet filter (firewall) must be implemented at minimum.

In the two-stage firewall architecture, all incoming and outgoing data traffic **MUST** be controlled and filtered by the external packet filter (firewall) or the internal packet filter (firewall).

A P-A-P structure consisting of a packet filter, an application layer gateway or security proxies and a packet filter **MUST** always be realised when required by the security policy or the requirement specification.

NET.1.1.A5 Client-Server Segmentation

Clients and servers **MUST** be placed in different security segments. The communication between these segments **MUST** be controlled by a stateful packet filter (firewall) at minimum.

It **SHOULD** be noted that possible exceptions which make it possible to position clients and servers in a shared security management are covered in the respective application- and system-specific modules.

For guest access and network areas where no internal control of the end devices is provided, dedicated security segments **MUST** be established.

NET.1.1.A6 End Device Segmentation in the Internal Network

The end devices positioned in a given security segment **MUST** correspond to a similar security level.

NET.1.1.A7 Protection of Sensitive Information

Sensitive information **MUST** be transmitted using protocols that are secure according to the state of the art in information security unless trusted dedicated network segments (e.g. within the management network) are used for communication. If it is not possible to use such protocols, appropriate encryption and authentication techniques according to the state of the art in information security **MUST** be implemented (see NET.3.3 VPN).

NET.1.1.A8 Basic Protection of Internet Access

Internet access **MUST** be implemented in accordance with NET.1.1.A4 *Network Separation in Security Zones*. Internet traffic **MUST** be routed via the firewall structure. The data flow **MUST** be restricted to the required protocols and communication relationships by the firewall structure.

NET.1.1.A9 Basic Protection of Communication with Untrusted Networks

The level of trustworthiness **MUST** be defined for every network. Networks that are not trusted at all **MUST** be treated like the Internet and secured accordingly.

NET.1.1.A10 DMZ Segmentation for Access from the Internet

The firewall structure **MUST** be complemented by a so-called external DMZ for all services and applications that can be accessed from the Internet. A concept for DMZ segmentation

SHOULD be drawn up that implements the security policy and the requirement specification in a transparent manner. Depending on the security level of the IT systems, the DMZ segments MUST be divided further. An external DMZ MUST be connected to the external packet filter.

NET.1.1.A11 Protection of Communications Entering the Internal Network from the Internet

IP-based access to the internal network MUST be granted via a secure communication channel and restricted to trusted IT systems and users (see NET.3.3 VPN). Such VPN gateways SHOULD be realised in an external DMZ. It SHOULD be noted that adequately hardened VPN gateways can be accessed directly from the Internet. All network access authenticated via the VPN gateway to the internal network MUST pass through the internal firewall at minimum (for protection of the internal network).

IT systems MUST NOT access the internal network via the Internet or the external DMZ. It SHOULD be noted that any exceptions from this requirement are covered in the relevant application- and system-specific modules (e.g. APP.5.1 *General Groupware*, NET.4.2 *VoIP*).

NET.1.1.A12 Protection of Outgoing Internal Communication to the Internet

Outgoing communication from the internal network to the Internet MUST be decoupled through a security proxy. The decoupling MUST be realised outside of the internal network. If P-A-P structure is in use, the outgoing communication SHOULD always be decoupled by the security proxies of the P-A-P structure.

NET.1.1.A13 Network Planning

Every network implementation MUST be planned in a suitable, comprehensive and transparent manner. In this context, the security policy and the requirement specification MUST be observed. In addition, the following aspects MUST be considered at minimum as required in the planning:

- the connection of the Internet and, if available, the local network and extranet
- the topology of the overall network and the network areas (i.e. security zones and segments)
- the capacity and redundancy of the network and security components, transmission routes and external connections
- the protocols to be used and their general configuration and addressing, in particular IPv4/IPv6 sub-networks of terminal device groups
- administration and monitoring (see NET.1.2 *Network Management*).

The network planning MUST be regularly reviewed.

NET.1.1.A14 Implementation of Network Planning

The planned network MUST be implemented properly. This MUST be verified during the approval process.

NET.1.1.A15 Regular Gap Analysis [Chief Information Security Officer (CISO)] (I)

Regular checks MUST be conducted to ensure that the existing network corresponds to the target condition. At minimum, the checks MUST identify the extent to which the security

policy and the requirement specification are met and the extent to which the implemented network structure corresponds to the current state of the network planning. To this end, responsible persons and test criteria or specifications **MUST** be defined.

Standard Requirements

For module NET.1.1 *Network Architecture and Design*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

NET.1.1.A16 Specification of Network Architecture

Based on the security policy and the requirement specification, an architecture for the security zones, including the internal network, DMZ area and external connections, **SHOULD** be developed and consistently maintained. In this context, all relevant architecture elements of the organisation **SHOULD** be taken into account, but the following are necessary at minimum:

- the architecture of the internal network with specifications on how network virtualisation technologies, layer 2 and layer 3 communication and redundancy procedures are to be used
- the network architecture for external connections, including firewall architectures, DMZ and extranet design and specifications for the site coupling
- specification of the network locations where security components such as firewall or IDS/IPS should be placed and which security functions they should provide
- specifications for the network connections of the different IT systems
- the network architecture in virtualisation hosts with a particular focus on network virtualisation overlays (NVOs) and the architecture in vertically integrated systems (ViS)
- specification of the basic architecture elements for a private cloud, as well as protection of the connections to virtual private clouds, hybrid clouds and public clouds (see OPS.3.2 *Cloud Providers* and OPS.3.4 *Managed Security Services*)
- architecture for secure administration and monitoring of the IT infrastructure

NET.1.1.A17 Specification of Network Design

Based on the network architecture, the network design for the security zones, including the internal network, the DMZ area and external connections, **SHOULD** be developed and consistently maintained. To this end, the relevant architecture elements **SHOULD** be detailed, but the following are necessary at minimum:

- admissible forms of network components, including virtualised network components
- specifications on how WAN and wireless connections should be protected
- the connection of end devices to switching components, connections between network elements and use of communication protocols
- redundancy mechanisms for all network elements
- an address concept for IPv4 and IPv6, as well as associated routing and switching concepts

- virtualised networks in virtualisation hosts, including NVO
- the structure, connection and protection of private clouds and the secure connection of virtual private clouds, hybrid clouds and public clouds
- specifications regarding network design for the secure administration and monitoring of the IT infrastructure

NET.1.1.A18 P-A-P Structure for the Internet Connection

A proxy-based application layer gateway (ALG) or corresponding security proxies **MUST** be realised between the two firewall stages (see NET.1.1.A4 *Network Separation in Security Zones*). These **MUST** be connected to the external firewall and the internal firewall via a transfer network (dual-homed). **ONLY** the proxy-based ALG or corresponding security proxies **MAY** be integrated in these transfer networks. All data traffic **MUST** be decoupled via the ALG or the corresponding security proxies. A transport network that connects both firewall stages with each other **MUST NOT** be configured. In addition, the internal firewall **MUST** reduce the number of possible points of attacks of the ALG or the security proxies for insiders or IT systems in the internal network.

Authenticated and trusted network access attempts from the VPN gateway to the internal network **SHOULD NOT** pass through the ALG or the security proxies of the P-A-P structure.

NET.1.1.A19 Separation of Infrastructure Services

Servers providing basic services for the IT infrastructure **SHOULD** be positioned in a dedicated security segment. The communication with these servers **SHOULD** be controlled by a stateful packet filter (firewall).

NET.1.1.A20 Allocation of Dedicated Sub-Networks for IPv4/IPv6 End Device Groups

Different IPv4-/IPv6 end devices **SHOULD** be allocated to dedicated sub-networks according to the protocol used (IPv4-/IPv6 or IPv4/IPv6 DualStack).

NET.1.1.A21 Separation of the Management Area

An out-of-band management scheme **SHOULD** be used continuously for managing the infrastructure. In this context, all end devices required for management of the IT infrastructure **SHOULD** be positioned in dedicated segments. The communication with these end devices **SHOULD** be controlled by a stateful packet filter (firewall). The communication from and to these management segments **SHOULD** be restricted to the necessary management protocols with defined communication end points.

The management area **SHOULD** comprise the following security segments at minimum, which **SHOULD** be divided further depending on the security policy and the requirement specification:

- segment(s) for IT systems that are responsible for the authentication and authorisation of the administrative communication
- segment(s) for administration of the IT systems
- segment(s) for monitoring

- segment(s) containing the central logging system, including the Syslog server and SIEM server
- segment(s) for IT systems required for basic services of the management area
- segment(s) for the management interface of the IT systems to be administrated.

The different management interfaces of the IT systems **MUST** be separated according to their purpose and their network position via a stateful packet filter (firewall). In addition, the following IT systems (management interfaces) **SHOULD** be separated via dedicated firewalls:

- IT systems that can be accessed from the Internet
- IT systems in the internal network
- security components located between the IT systems accessible from the Internet and the internal network

It **MUST** be ensured that the segmentation cannot be circumvented by the management communication; this means that the possibility of bypassing segments **MUST** be excluded.

NET.1.1.A22 Specification of the Segmentation Concept

Based on the specifications of the network architecture and network design, a comprehensive segmentation concept for the internal network, including any existing virtualised networks in virtualisation hosts, **SHOULD** be planned, implemented and consistently maintained. The concept **SHOULD** comprise the following aspects at minimum, assuming they are planned in the target environment:

- security segments to be created initially, as well as specifications on how new security segments are to be created and how end devices are to be positioned in the security segments
- specification for the segmentation of development and test systems (staging)
- network access control for security segments with clients
- connection of network areas which are connected to the security segments via wireless technologies or a dedicated line
- connection of the virtualisation hosts and virtual machines on the hosts to the security segments
- data centre automation
- specifications on how end devices that supply several security segments are to be included (e.g. load balancers and storage and backup solutions)

Depending on the security policy and the requirement specification, a concept **SHOULD** be developed that describes how each security segment is to be implemented in networking terms. In addition, it **SHOULD** be defined which security functions must be provided by the coupling elements between the security segments (e.g. a firewall as a stateful packet filter or IDS/IPS).

NET.1.1.A23 Separation of Security Segments

IT systems with different protection needs SHOULD be placed in different security segments. If this is not possible, the protection needs are to follow the highest protection needs of a given security segment. In addition, the security segments SHOULD be further divided depending on their size and the requirements of the segmentation concept. It MUST be ensured that it is not possible to bypass segments, or even zones.

If the VLANs on a switch belong to different organisations, the separation SHOULD be implemented physically or encryption SHOULD be used to protect the information transmitted from unauthorised access.

NET.1.1.A24 Secure Logical Separation via VLAN

It MUST NOT be possible for a virtual LAN (VLAN) to establish a connection between a zone before the ALG or the security proxies of a P-A-P structure and the internal network located behind it.

In general, it MUST be ensured that it is not possible to bypass zones when using VLANs.

NET.1.1.A25 Detailed and Implementation Planning of Network Architecture and Design

Detailed and implementation planning for the network architecture and design SHOULD be carried out, documented, reviewed and consistently maintained.

NET.1.1.A26 Specification of Operational Processes for the Network

To ensure secure and effective network operations, operational processes SHOULD be created or adapted based on the actual needs and documented (see the module group Core IT Operation, in particular OPS.1.1.3 *Patch and Change Management*). In this context, it SHOULD be considered in particular how the zoning and the segmentation concept affects the IT operations.

NET.1.1.A27 Integration of Network Architecture into Contingency Planning [Head of IT]

Transparent analyses SHOULD be carried out initially and at regular intervals to determine how the network architecture and the derived concepts affect the contingency planning.

Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.1.1 *Network Architecture and Design* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

NET.1.1.A28 High-Availability Network and Security Components (A)

Central areas of the internal network, as well as the security components, SHOULD be realised with high availability. To this end, the components SHOULD be designed redundantly and realised with high internal availability, as well.

NET.1.1.A29 High-Availability Realisation of Network Connections (A)

The network connections (e.g. the Internet connection and WAN connections) SHOULD be designed with full redundancy. Depending on the availability requirements, redundant connec-

tions to one or different providers SHOULD be implemented with different technology and performance as needed. Redundant routes SHOULD also be implemented both within and outside of the organisation's purview as needed. To this end, possible single points of failure (SPoF) and disruptive environmental conditions SHOULD be considered.

NET.1.1.A30 Protection Against Distributed Denial of Service (A)

In order to fend off DDoS attacks, the available bandwidth SHOULD be purposefully distributed over different communication partners and protocols by means of bandwidth management.

In order to be able to fend off DDoS attacks with very high data rates, mitigation services SHOULD be purchased via larger Internet service providers (ISPs) and their use SHOULD be contractually regulated.

NET.1.1.A31 Physical Separation of Security Segments (CIA)

Depending on the security policy and requirement specification, security segments SHOULD be physically separated by separate switches.

NET.1.1.A32 Physical Separation of Management Segments (CIA)

Depending on the security policy and requirement specification, security segments of the management area SHOULD be physically separated from each other.

NET.1.1.A33 Micro-Segmentation of the Network (CIA)

To restrict potential attacks to a small number of end devices, the network SHOULD be divided into small segments with very similar requirement profiles and the same protection needs. This SHOULD be considered for the DMZ segments in particular.

NET.1.1.A34 Use of Cryptographic Methods at the Network Level (CI)

The security segments SHOULD already be realised at the network level in the internal network, the extranet and the DMZ area by means of cryptographic techniques. To this end, VPN techniques or IEEE 802.1AE SHOULD be used.

If communication within the internal network or DMZ takes place via transmission routes which are not sufficiently secure for increased protection needs, the communication SHOULD be adequately encrypted at the network level.

NET.1.1.A35 Use of Network-Based DLP [Chief Information Security Officer (CISO)] (CI)

Systems for data loss prevention (DLP) SHOULD be used at the network level to reduce the risk of data leakage.

NET.1.1.A36 Separation by Means of VLAN for Very High Protection Needs (CIA)

If the protection needs are very high, VLANs SHOULD NOT be used.

Additional Information

For more information about threats and security safeguards for module NET.1.1 *Network Architecture and Design*, see the following publications, among others:

[27033-5]	ISO/IEC 27033-5:2013: Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs), International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, August 2013
[ISILANA]	Secure Connection of Local Networks to the Internet (ISi-LANA): Federal Office for Information Security (BSI), Version 2.1, August 2014 https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html , last accessed on 05.10.2018
[TL2103]	Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf [Technical Guideline for Internal Organisation of Telecommunication Systems with Increased Protection Needs]: BSI-TL-02103 - Version 2.0, Federal Office for Information Security (BSI), 2014, https://www.bsi.bund.de/DE/Publikationen/TL-sichere-TK-Anlagen/TL02103_hm.html , last accessed on 05.10.2018
[TR21022]	Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths: Part 2: Use of Transport Layer Security (TLS), Federal Office for Information Security (BSI), January 2017, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_hm.html , last accessed on 24.08.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.1.1 *Network Architecture and Design*:

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.39 Malware

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

Elementary Threats Requirements	G 0.9	G 0.11	G 0.18	G 0.19	G 0.22	G 0.23	G 0.27	G 0.29	G 0.30	G 0.39	G 0.40	G 0.43
NET.1.1.A1	X	X	X	X	X	X	X	X	X	X	X	X
NET.1.1.A2			X				X	X				
NET.1.1.A3	X	X	X	X	X	X	X		X	X	X	X
NET.1.1.A4	X		X	X		X		X	X	X	X	X
NET.1.1.A5	X			X	X	X		X	X	X	X	X
NET.1.1.A6	X			X	X	X		X	X	X		X
NET.1.1.A7				X	X	X		X				X
NET.1.1.A8			X	X	X	X		X	X	X	X	X
NET.1.1.A9			X	X	X	X		X	X	X	X	X
NET.1.1.A10			X	X	X	X		X	X	X	X	X
NET.1.1.A11			X	X	X	X		X	X	X	X	X
NET.1.1.A12			X	X		X		X	X	X		
NET.1.1.A13	X	X	X	X	X	X	X	X	X	X	X	X
NET.1.1.A14	X	X	X	X	X	X	X	X	X	X	X	X
NET.1.1.A15	X		X				X	X	X			
NET.1.1.A16	X	X	X	X	X	X	X	X	X	X	X	X
NET.1.1.A17	X	X	X	X	X	X	X	X	X	X	X	X
NET.1.1.A18	X		X	X	X	X		X	X	X	X	X
NET.1.1.A19	X			X	X	X			X	X	X	X
NET.1.1.A20	X		X				X					
NET.1.1.A21	X		X		X	X			X	X		X

NET.1.1.A22	X		X	X	X	X	X		X	X	X	X
NET.1.1.A23	X		X	X	X	X			X	X	X	X
NET.1.1.A24	X		X	X	X	X			X			X
NET.1.1.A25	X	X	X	X	X	X	X	X	X	X	X	X
NET.1.1.A26	X		X						X			
NET.1.1.A27	X	X	X					X		X	X	
NET.1.1.A28	X	X					X				X	
NET.1.1.A29	X	X					X				X	
NET.1.1.A30	X	X					X				X	
NET.1.1.A31	X		X	X	X	X				X	X	X
NET.1.1.A32					X	X			X			
NET.1.1.A33	X			X	X	X			X	X		X
NET.1.1.A34				X	X	X		X	X	X		X
NET.1.1.A35				X	X	X		X	X	X	X	
NET.1.1.A36	X		X	X	X	X			X			X



NET.1.2: Network Management

Description

Introduction

Reliable network management is a basic requirement for securely and efficiently operating state-of-the-art networks. To make this possible, network management must comprehensively integrate all network components and implement appropriate safeguards in order to protect the management communication and infrastructure.

Network management includes many important functions, such as network monitoring, configuration of the components, event handling and logging. Another important function is reporting, which may be designed as a common platform for network and IT systems. Alternatively, it may be implemented in a dedicated manner as a uniform platform or as part of the individual management components.

The network management infrastructure consists of central management systems (e.g. SNMP servers); administration end devices (including software for management access), decentralised management agents, dedicated management tools (e.g. probes and specific instruments), management protocols (e.g. SNMP or SSH) and management interfaces (e.g. dedicated Ethernet ports or console ports).

Objective

The objective of this module is to establish information security as an integral part of network management.

Not in Scope

This module considers the necessary components and conceptual tasks involved in network management. The analogous aspects of system management for networked clients and servers are described in module OPS.1.1.7 *Network and System Management*.

This module adds further details to the basic requirements contained in module NET.1.1 *Network Architecture and Design*. Furthermore, it addresses how network management can be structured and protected and how the related communication can be protected. However, details regarding the protection of network components, particularly their management interfaces, are covered by the module groups NET.2 and NET.3.

The process of managing the passive network infrastructure is addressed in the modules on infrastructure (INF module layer) and industrial IT (IND module layer). As a consequence, these subjects are not described within the framework of this module.

The logging addressed in this module should be integrated into a comprehensive logging and archiving concept (see OPS.1.1.5 *Logging*).

The present module does not address the subject of outsourcing in detail. Further requirements in this regard are described in module OPS.2.1 *Outsourcing for Customers*.

General aspects regarding secure, efficient and controlled operation of network management are only described within the framework of this module in cases where they go beyond the general requirements of module OPS.1.1.1 *General IT Operation*.

Threat Landscape

For module NET.1.2 *Network Management*, the following specific threats and vulnerabilities are of particular importance:

Unauthorised Access to Central Network Management Components

If attackers manage to access network management solutions (e.g. due to unpatched vulnerabilities or insufficient network separation), they can control and reconfigure all connected network components. They may thus access sensitive information, divert network traffic or even significantly disrupt the entire network.

Unauthorised Access to Individual Network Components

If attackers manage to gain access to individual network components, they can control and manipulate the respective component. All data traffic that passes through the network component may be compromised as a consequence. Furthermore, additional attacks may be prepared in order to increase the depth of penetration of the organisation's network.

Unauthorised Interference in Network Management Communication

If management communication is intercepted and manipulated, active network components can be configured improperly and controlled. This may violate the network integrity and limit the availability of the network infrastructure. Furthermore, the data transmitted may be intercepted and viewed.

Insufficient Time Synchronisation of Network Management Components

If the system time of the network management components is synchronised insufficiently, the logging data might not correlate or the correlation may result in incorrect statements due to the lack of a common basis among the different time stamps of events. As a consequence, it will not be possible to react appropriately to events and eliminate issues. Security incidents and data leaks may thus remain undetected.

Requirements

The specific requirements of module NET.1.2 *Network Management* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must also always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security policies defined. There can be additional roles with further

responsibilities for the implementation of requirements. These roles are listed in square brackets in the header of the respective requirement.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO), Head of Networks, Head of IT, Supervisor

Basic Requirements

For module NET.1.2 *Network Management*, the following requirements **MUST** be implemented as a matter of priority:

NET.1.2.A1 Network Management Planning

The network management infrastructure **MUST** be planned appropriately. In so doing, all items addressed in the security policy and requirements specification and the role concept and access control policy **SHOULD** be taken into account. At minimum, the following aspects **MUST** be taken into account:

- management areas to be separated
- access options for the management server
- communication for management access
- protocols used (e.g. IPv4 and IPv6)
- requirements for management tools
- interfaces for forwarding collected event or alarm messages
- logging (including required interfaces to a centralised logging solution)
- reporting and interfaces to comprehensive solutions
- corresponding requirements for the network components to be integrated

NET.1.2.A2 Specification of Network Management Requirements [Head of IT]

Based on NET.1.2A1 *Network Management Planning*, requirements for the network management infrastructure and processes **MUST** be specified. In so doing, all essential elements of network management **MUST** be taken into account. The network management policy **SHOULD** also be considered.

NET.1.2.A3 Role Concept and Access Control Policy for Network Management

A role concept and access control policy for network management **MUST** be drawn up, implemented and maintained. The concept **MUST** map the specific activities and the related access to information in network management.

NET.1.2.A4 Basic Authentication for Network Management Access [Head of IT, Chief Information Security Officer (CISO)] (I)

Appropriate authentication **MUST** be used for management access to network components and management information. To this end, the specifications of the organisation regarding authentication quality and the handling of authentication information **MUST** be implemented. All default passwords on the network components **MUST** also be changed. The new passwords **MUST** be sufficiently strong and changed at regular intervals.

NET.1.2.A5 Installing Updates and Patches

The employees in charge **MUST** regularly obtain information on any vulnerabilities that have become known in the network management solutions deployed and install security updates and patches as quickly as possible. Updates that are not relevant for security **MUST NOT** impair the security and stability of the network management solution.

NET.1.2.A6 Regular Backups

All network management solutions used **MUST** be integrated into the organisation's backup concept (see CON.3 *Backup Concept*). In so doing, all specific data for network management **MUST** be taken into account. At minimum, the system data for integrating the components or objects to be managed, event messages, statistical data and stored data for configuration management **MUST** be backed up.

NET.1.2.A7 Basic Logging of Events

The network management solution **MUST** be integrated into the logging concept of the organisation (see OPS.1.1.5 *Logging*). Furthermore, the following events **MUST** be logged at minimum: unauthorised access (all attempts), fluctuations in network performance or availability, errors in automatic processes (e.g. regarding configuration distribution) and limited availability of network components.

NET.1.2.A8 Time Synchronisation

All network management components, including the integrated network components, **MUST** be synchronised. The time **MUST** be synchronised by means of the NTP service at every location within the local network. If a separate management network has been established, an NTP instance **MUST** be positioned within it.

NET.1.2.A9 Protection of Network Management Communication

If the network management communication takes place via the production infrastructure, secure, state-of-the-art protocols **MUST** be used. If this is not possible, a dedicated administration network (out-of-band management) **MUST** be used (see NET.1.1 *Network Architecture and Design*).

NET.1.2.A10 Limitation of SNMP Communication

In network management, insecure versions of the Simple Network Management Protocol (SNMP) **MUST NOT** be used. However, if this is not possible, the SNMP communication **MUST** either be performed using a separate management network or SNMPv3 **MUST** be used with authentication and encryption. As a matter of principle, SNMP **SHOULD ONLY** be used for access with the minimum access rights required. The access authorisations **SHOULD** be limited to dedicated management servers.

Standard Requirements

For module NET.1.2 *Network Management*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

NET.1.2.A11 Definition of a Security Policy for Network Management [Chief Information Security Officer (CISO)]

For network management, a security policy SHOULD be drawn up and continuously maintained. The policy SHOULD be known to all persons involved in network management and SHOULD be the basis of their work. Regular and transparent reviews SHOULD be conducted to ensure that the policy requirements are being implemented. The results MUST be documented in an appropriate manner.

The security policy SHOULD define which areas of network management are to be implemented using central management tools and services. It SHOULD also define the extent to which tasks in the network management of the organisation are to be implemented automatically.

Moreover, framework conditions and specifications for network separation, access control, logging, and the protection of communications, the network management tools, and the basic operative rules for network management SHOULD be specified.

NET.1.2.A12 Current Inventory and Documentation of Network Management

Documentation SHOULD be drawn up that describes the management infrastructure of the network. It SHOULD include the initial actual situation and all changes made in network management. In particular, it SHOULD document which network components are administered using which management tools. Furthermore, all IT workstations and end devices used for network management, as well as the entire stock of information and management data on network management operations, SHOULD be included. Finally, all interfaces to applications and services outside of network management SHOULD be documented.

The resulting documentation of the actual situation of the management infrastructure SHOULD be compared against the network infrastructure documentation (see module NET.1.1 *Network Architecture and Design*).

The documentation MUST be complete and up to date at all times.

NET.1.2.A13 Drawing Up a Network Management Concept [Head of IT]

Based on the security policy (see NET.1.2.A11 *Defining a Security Policy for Network Management*), a network management concept SHOULD be drawn up and continuously maintained. In doing so, the following minimum aspects SHOULD be taken into account as required:

- methods, techniques, and tools for network management
- protection of access and communication
- network separation (in particular, the assignment of network management components to security zones)
- the scope of monitoring and alarming for each network component

- logging
- automation (particularly of the central distribution of configuration files to switches)
- reporting chains in the event of malfunctions and security incidents
- provisioning of network management information for other areas of the company
- integration of network management into contingency planning

NET.1.2.A14 Detailed and Implementation Planning

Detailed and implementation planning for the network management infrastructure SHOULD be drawn up. In so doing, all items addressed in the security policy and the network management concept SHOULD be addressed.

NET.1.2.A15 Concept for Secure Operation of the Network Management Infrastructure

Based on the security policies and the network management concept, a concept for secure operation of the network management infrastructure SHOULD be drawn up. This concept SHOULD take into account the application and system operations for the network management tools. It SHOULD also be checked how the performance of other operative units can be integrated and controlled.

NET.1.2.A16 Setup and Configuration of Network Management Solutions

Network management solutions SHOULD be established, configured securely and commissioned based on the security policy (see NET.1.2.A11 *Defining a Security Policy for Network Management*), the specific requirements (see NET.1.2.A2 *Specification of Network Management Requirements*) and the detailed and implementation plan. Afterwards, the specific processes for network management SHOULD be set up.

NET.1.2.A17 Regular Gap Analysis

The extent to which the network management solution corresponds to the target state SHOULD be checked regularly and transparently. In so doing, it SHOULD be checked whether the existing solution still complies with the security policy and requirements specification. The extent to which the management structure implemented and the processes used comply with the current status SHOULD also be checked. Moreover, the management infrastructure SHOULD be compared against the latest state-of-the-art technology.

NET.1.2.A18 Training for Management Solutions [Head of IT, Supervisor]

Training programs SHOULD be developed and carried out for the network management solutions used. The measures SHOULD cover the individual circumstances in configuration, availability and capacity management, as well as typical situations in the field of error management. The training SHOULD be repeated at regular intervals, but at least when there are major technical or organisational changes within the network management solutions.

NET.1.2.A19 Strong Authentication for Management Access

An authentication method corresponding to the state of the art SHOULD be used for administrative access to network components. Administrative access SHOULD be authenticated via a central authentication server with the help of personalised accounts and correspondingly secure protocols.

NET.1.2.A20 Protection of Access to Network Management Solutions

Access to central network management solutions and management information SHOULD be protected by a state-of-the-art authentication method. This access SHOULD be authenticated via a central authentication server with the help of personalised accounts.

State-of-the-art authentication and encryption methods MUST be implemented if network management tools are accessed from a network outside of the management networks, particularly in cases involving a production network or an insufficiently protected network.

NET.1.2.A21 Decoupling of Network Management Communication

An administrator SHOULD NOT be able to access a network component directly from an IT system outside of the management networks. If such access is necessary without a central management tool, the communication SHOULD be decoupled. Jump servers of this kind SHOULD be integrated into the management network and located in a separate access segment.

NET.1.2.A22 Restricting Management Functions

Only the services needed SHOULD be enabled.

NET.1.2.A23 Logging Administrative Access

Within the framework of network management, the session data of all instances of administrative access SHOULD be logged and stored. In so doing, the data protection regulations SHOULD be taken into consideration.

The logging data SHOULD be protected sufficiently and according to the laws in backups. Furthermore, it SHOULD be defined whether and to what extent session data must be archived for forensic analyses. If data is archived, it SHOULD be ensured that this is performed according to the laws and in an audit-compliant manner.

NET.1.2.A24 Central Configuration Management for Network Components

It SHOULD be possible to automatically distribute, install and activate software, firmware, configuration data and network components over the network without interrupting operations. The information required in this regard SHOULD be securely available from a central location and integrated into version management and backup processes. The central configuration management SHOULD be maintained continuously and audited regularly.

NET.1.2.A25 Status Monitoring for Network Components

The basic performance and availability parameters of the central network components SHOULD be monitored continuously. To this end, the respective threshold values SHOULD be determined in advance (baselining).

NET.1.2.A26 Comprehensive Logging, Alarming and Documentation of Events

Important events and error conditions SHOULD be transferred automatically to a central management system and logged therein. This applies to events on both network components and network management tools. In addition, the IT personnel in charge SHOULD be informed automatically. Alarming and logging SHOULD include the following items at minimum:

- failure and non-availability of network or management components

- hardware malfunctions
- failed login attempts
- critical conditions or overloading of IT systems

Event messages and logging data SHOULD be transmitted continuously or cumulatively to a central management system. Alarm messages SHOULD be transmitted directly as they occur.

NET.1.2.A27 Integration of Network Management into Contingency Planning

The network management solutions SHOULD be integrated into the organisation's contingency planning. To this end, the network management tools and the configurations of the network components SHOULD be backed up and integrated into the recovery schemes.

NET.1.2.A28 Location of Management Clients for In-Band Management

For administrating both the internal and external IT systems, dedicated management clients SHOULD be used. To this end, one management client MUST be located on the external network area (for administrating IT systems connected to the Internet) and another in the internal area (for administrating internal IT systems).

NET.1.2.A29 Using VLANs in the Management Zone

If management networks are separated by VLANs, it SHOULD be ensured that the external packet filter and the devices connected to this filter are located in their own sub-network. It MUST also be ensured that the ALG is not bypassed in this process.

Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.1.2 *Network Management* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

NET.1.2.A30 High-Availability Implementation of the Management Solution (A)

Central management solutions SHOULD be operated in a highly available manner. To this end, the servers and tools (including the network connections) SHOULD be designed redundantly. The individual components SHOULD also be provided in a highly available manner.

NET.1.2.A31 Basic Use of Secure Protocols (CIA)

Only secure protocols SHOULD be used for network management. All security features of these protocols SHOULD be used.

NET.1.2.A32 Physical Separation of Security Segments (CIA)

The management network SHOULD be separated physically.

NET.1.2.A33 Physical Separation of Management Segments [Head of Networks] (CIA)

The management network SHOULD be divided into physically separated security zones. In so doing, physically separated security zones SHOULD be established at minimum for managing LAN components, security components and components for external connections.

NET.1.2.A34 Logging of Administrative Session Content (CI)

In addition to logging session data (see NET.1.2.A22 *Logging Administrative Access*), administrative access content SHOULD be logged. Alternatively, the principle of dual control SHOULD be followed. The logged contents of the administrative sessions SHOULD also be protected sufficiently and according to the laws in backups.

NET.1.2.A35 Specifications for Securing Evidence (CIA)

Procedures for securing evidence and forensic investigations within the framework of network management SHOULD be defined and documented. The logged data collected SHOULD be archived for forensic analyses according to the laws and in an audit-compliant manner.

NET.1.2.A36 Integration of Network Management Logging into an SIEM Solution (CIA)

Network management logging SHOULD be integrated into a security information and event management (SIEM) solution. To this end, the requirements catalogues (see NET.1.2.A2) for selecting network management solutions SHOULD be adapted in terms of the necessary support of interfaces and transmission formats.

NET.1.2.A37 Time Synchronisation Across Locations (CI)

Time synchronisation SHOULD be ensured across all locations of the organisation. To this end, a common reference time SHOULD be used (e.g. using a superior NTP server).

NET.1.2.A38 Specification of Forms of Emergency Operations for the Network Management Infrastructure (A)

In order to quickly recover the target conditions of software and firmware and configure the components in the network management infrastructure, sufficient replacement solutions SHOULD be defined that may be used to perform the administrative activities in the event of an emergency.

Additional Information

For more information about threats and security safeguards for module NET.1.2 *Network Management*, see the following publications, among others:

[ISI]	BSI Standards on Internet Security (ISi series): https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Reihe_node.html , last accessed on 05.10.2018
[TR21022]	Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths: Part 2: Use of Transport Layer Security (TLS), Federal Office for Information Security (BSI), January 2017, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , last accessed on 24.08.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.1.2 *Network Management*:

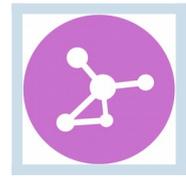
G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

- G 0.14 Interception of Information / Espionage
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.25 Failure of Devices or Systems
- G 0.27 Lack of Resources
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.39 Malware
- G 0.40 Denial of Service
- G 0.43 Attack with Specially Crafted Messages

Elementary Threats Requirements	G 0.9	G 0.11	G 0.14	G 0.18	G 0.19	G 0.22	G 0.23	G 0.25	G 0.27	G 0.29	G 0.30	G 0.39	G 0.40	G 0.43
NET.1.2.A1			X	X	X	X	X	X		X	X		X	X
NET.1.2.A2	X	X	X	X	X	X	X	X	X	X	X	X	X	X
NET.1.2.A3			X		X	X				X	X			X
NET.1.2.A4			X		X	X				X	X			X
NET.1.2.A5			X	X	X	X	X				X	X	X	X
NET.1.2.A6			X		X	X	X		X				X	X
NET.1.2.A7		X			X	X				X	X	X	X	
NET.1.2.A8	X		X			X	X	X						
NET.1.2.A9	X		X		X	X	X	X	X	X	X	X	X	X
NET.1.2.A10			X			X	X				X	X	X	X
NET.1.2.A11			X	X	X	X	X	X		X	X		X	X
NET.1.2.A12	X			X					X	X				
NET.1.2.A13	X	X	X	X	X	X	X	X		X	X		X	
NET.1.2.A14	X	X	X	X	X	X	X	X	X	X	X	X	X	X
NET.1.2.A15	X							X	X					
NET.1.2.A16	X	X		X			X	X	X	X	X			
NET.1.2.A17				X			X		X	X				
NET.1.2.A18	X			X	X		X			X				
NET.1.2.A19			X		X	X	X			X	X	X	X	X
NET.1.2.A20			X		X	X	X				X	X	X	X
NET.1.2.A21			X		X	X	X				X	X	X	X

NET.1.2.A22			X		X	X	X				X			
NET.1.2.A23	X	X		X	X	X	X			X	X	X		
NET.1.2.A24	X			X				X						
NET.1.2.A25	X	X		X			X	X	X				X	
NET.1.2.A26	X	X					X	X	X		X	X	X	X
NET.1.2.A27	X	X						X						
NET.1.2.A28	X			X			X				X			
NET.1.2.A29			X		X		X				X			
NET.1.2.A30	X	X		X				X	X				X	
NET.1.2.A31			X		X	X	X			X	X	X	X	X
NET.1.2.A32	X		X		X	X	X	X	X	X	X	X	X	X
NET.1.2.A33	X		X		X	X	X			X	X	X	X	X
NET.1.2.A34						X	X			X	X			X
NET.1.2.A35				X	X	X	X			X	X	X	X	X
NET.1.2.A36	X		X	X	X	X	X	X		X	X	X	X	X
NET.1.2.A37	X	X	X			X	X	X						
NET.1.2.A38	X	X		X				X					X	



NET.2.1: WLAN Operation

Description

Introduction

Wireless LANs (WLANs) can be used to create wireless local networks or extend existing wired networks. Up to now, almost all WLAN components available on the market have been based on the IEEE 802.11 standard and its additions. The Wi-Fi Alliance, a consortium of companies, plays an important role in this regard as the creator of the industry-agreed “Wi-Fi” standard based on IEEE 802.11. The Wi-Fi Alliance uses the Wi-Fi quality label to confirm that a device has passed certain interoperability and conformity tests.

Due to the frequently simple installation, WLANs are also used for temporarily establishing networks – for example, at trade fairs or smaller events. Furthermore, network access may be offered in public spaces such as airports or train stations through hotspots. This enables the mobile users to connect to the Internet or to their company network. Communication generally takes place between a central point of access, the access point and the WLAN component of the end device (i.e. using a WLAN USB adapter or an integrated WLAN feature).

Objective

This module seeks to systematically show how WLANs can be established and operated securely in an organisation.

Not in Scope

The module includes basic requirements that must be considered and met when establishing and operating WLANs. Requirements for the secure use of WLANs are not part of the present module. The secure use of WLANs is addressed in module NET.2.2 *WLAN Usage*. The operation of hotspots (see NET.2.3 *Operation of Hotspots*) is not detailed herein either.

WLANs may be operated in two different modes depending on the needs of an operator and the hardware equipment available. In ad-hoc mode, two or more mobile end devices equipped with a WLAN network card communicate directly with each other. Since WLANs in ad-hoc mode can establish and configure themselves (i.e. without any stationary infrastructure) and are thereby able to establish a fully meshed parallel network infrastructure, ad-hoc mode is not appropriate in environments that require protection. This mode is not considered further below. In the majority of cases, WLANs are operated in infrastructure mode (i.e. the client communication and the connection to wired LAN segments is carried out via the access point).

Threat Landscape

For module NET.2.1 *WLAN Operation*, the following specific threats and vulnerabilities are of particular importance:

Failure or Disruption of a Radio Network

In radio networks, information is transmitted using electromagnetic radio waves. If there are other electromagnetic sources radiating energy in the same frequency spectrum, these emissions could disrupt wireless communication and, in extreme cases, prevent the operation of the WLAN. This may be caused by other radio systems and devices such as Bluetooth, microwave ovens, or other WLAN networks. Denial-of-service attacks are possible as well. For example, if certain control and management signals are sent repeatedly, this may hinder the availability of the radio network.

Non-Existent or Inadequate Planning of WLAN Usage

Planning errors often turn out to be particularly serious because they may easily create extensive vulnerabilities. If the use of WLANs is planned insufficiently (or not at all), this may result in a number of issues, such as the following:

- Confidential data might be intercepted – for example, when using WLAN standards that no longer correspond to the state of the art (e.g. WEP for encryption).
- The transmission capacity may be insufficient. As a consequence, it will not be possible to use bandwidth-intensive applications with the required service quality.

Non-Existent or Insufficient Rules for WLAN Usage

If a WLAN infrastructure is not administered centrally, the access points in the default setting will mostly be pre-configured with insufficient security mechanisms (or none at all). For example, if an employee connects an unauthorised or insecure access point to an internal network of the organisation due to a lack of rules, the employee will undermine practically all the security safeguards implemented in the LAN, including the security gateway (firewall) used to protect against unauthorised external access.

Inappropriate Selection of Authentication Methods

If authentication methods or mechanisms are missing or inadequate, this may result in vulnerabilities. For example, the IEEE 802.1X (Port-Based Network Access Control) standard defines the EAP (Extensible Authentication Protocol). Some of the EAP methods described include vulnerabilities; EAP-MD5, for example, is susceptible to man-in-the-middle and dictionary attacks. If EAP-MD5 is being used, passwords might be guessed and eavesdropping could take place.

Incorrect Configuration of WLAN Infrastructure

Access points and other WLAN components (e.g. WLAN controllers) provide numerous configuration settings that relate in particular to security features. If the settings performed here are incorrect, communication via an access point will be impossible or insufficiently protected (if at all).

Non-Existent or Insufficient WLAN Security Mechanisms

In their delivered configurations, WLAN components are often configured with only a few security mechanisms activated (or none at all). Some of these mechanisms also fail to offer adequate protection. Even today, various WLAN components are used that only support inadequate security mechanisms such as WEP. In some cases, these devices cannot even be updated with stronger security mechanisms. If such devices are being used, an attacker might easily eavesdrop on all communications and thereby obtain confidential information.

Eavesdropping on WLAN Communication

Since radio is a medium that can be shared by several users, the data transmitted via WLANs can easily be intercepted and recorded. If the data is insufficiently encrypted (or not at all), transmitted payloads can easily be obtained. Furthermore, wireless networks and the radio waves emitted often radiate beyond the rooms in which the networks are used, making it possible for data to be sent to areas which cannot be controlled and secured by the users or an organisation.

Simulating a Valid Access Point (Rogue Access Points)

An attacker can masquerade as a part of the WLAN infrastructure by installing their own access point with a suitable SSID in the vicinity of a client. A simulated access point of this kind is referred to as a “rogue access point”. If this access point provides the WLAN client with stronger transmission performance than the real access point, the client will use it as its base station if mutual authentication is not enforced. Furthermore, the real access point may be disabled by a denial-of-service attack. The users log into a network that only pretends to be the target network. This makes it possible for an attacker to eavesdrop on communications. Poisoning or spoofing methods can also simulate a false identity for an attacker or redirect the network traffic to the attacker's systems. This means that the attacker can listen in on and control communications. Particularly in public radio networks (so-called hotspots), a rogue access point is a frequently used means of attack.

Unprotected LAN Access at the Access Point

If access points are mounted visibly and without any physical protection, an attacker may position themselves between the access points and the switch infrastructure in order to eavesdrop on all the network traffic. Even if communications are encrypted using WPA2, this presents a risk because these methods only protect the air interface and do not take the Ethernet connection into account.

Hardware Damage

Hardware damage may cause disruptions in radio traffic. In the worst-case scenario, the WLAN might even fail completely. This is particularly applicable to WLAN devices mounted outside of protected rooms (e.g. in order to cover open spaces). They are exposed to additional threats such as deliberate damage caused by attackers or environmentally related damage caused by lightning or other weather.

Theft of an Access Point

If unprotected WLAN access points are mounted in areas where people pass by (e.g. directly below the ceiling or in crowded areas), they might be stolen. As a consequence, a shared secret key for authentication to the RADIUS server or another key used (such as for WPA2 Personal) may

be read out, for example. This information may be used in order to access the WLAN without authorisation.

Requirements

The specific requirements of module NET.2.1 *WLAN Operation* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Planner, Head of IT, Building Services

Basic Requirements

For module NET.2.1 *WLAN Operation*, the following requirements **MUST** be implemented as a matter of priority:

NET.2.1.A1 Definition of a Strategy for WLAN Usage [Head of IT]

Before WLANs are used in an organisation, the organisation's general strategy for WLAN usage **MUST** be specified. In particular, it **MUST** be clarified and defined which organisational units, which applications, and what purpose WLANs will be used in/for, as well as which information may be transmitted. The spatial areas in which WLANs are to be established **MUST** also be defined.

Furthermore, it **MUST** already be defined in the planning phase who will be responsible for the administration of the various WLAN components, which interfaces will be in place between the persons in charge who are involved in operations, and when which information must be exchanged between the persons in charge.

NET.2.1.A2 Selection of a Suitable WLAN Standard [Planner]

In order to avoid inherent WLAN errors, it **MUST** initially be determined within the framework of WLAN planning which of the systems operated by the organisation (e.g. microwave ovens, Bluetooth) radiate into the ISM band at 2.4GHz and into the 5GHz band.

In addition, the security mechanisms available in the individual WLAN standards **MUST** be compared. In general, it **MUST** be ensured that only authentication and encryption methods will be used that are generally considered secure. Only after the individual standards have been evaluated in detail can a certain WLAN standard be defined. The reasons on which the decision is based **MUST** be documented.

Devices that need to fall back on insecure methods from recognised secure methods **MUST NOT** be considered during planning.

NET.2.1.A3 Selection of Suitable Crypto Methods for WLAN [Planner]

In order to securely operate a WLAN, all communication via the air interface **MUST** be encrypted. Cryptographic methods that are more insecure than WPA2 **MUST NOT** be used.

If WPA2 is used with pre-shared keys (WPA2-PSK), a complex key with a minimum length of 20 characters **MUST** be used. In addition, this key **MUST** be changed regularly.

NET.2.1.A4 Suitable Location of Access Points [Building Services]

Access points **MUST** be mounted such that they cannot be accessed. Furthermore, it **MUST** be ensured that the emission of radio waves into areas not designated for WLAN coverage is reduced as much as possible. External installations **MUST** be protected appropriately against weather and electrical discharges (e.g. lightning strikes).

NET.2.1.A5 Secure Basic Configuration of Access Points

Access points **MUST NOT** be used in their default configuration. Pre-set SSIDs (service set identifiers), passwords and cryptographic keys **MUST** be changed immediately upon completion of the commissioning process. Furthermore, insecure administration access (e.g. Telnet or HTTP) **MUST** be deactivated. Access points **MUST** be administered in an encrypted manner.

NET.2.1.A6 Secure Configuration of WLAN Clients

In order to be able to securely operate an internal WLAN infrastructure, all WLAN clients linked to it **SHOULD** be configured securely as well. Appropriate requirements for the secure configuration of clients can be found in module *SYS.2.1 General Client* and *NET.2.2 WLAN Usage*. In addition, the following WLAN-specific requirements **MUST** be met:

- If the WLAN interface is not used over extended periods of time, it **MUST** be disabled.
- It **MUST** be ensured that the WLAN communication is not used to couple security zones or bypass established protection safeguards.

NET.2.1.A7 Setting Up a Distribution System [Planner]

If a distribution system is established, a basic decision **MUST** be made as to whether separation will be performed physically or logically through VLANs on the access switches of the wired LAN.

NET.2.1.A8 Procedures in the Event of WLAN Security Incidents

In the event of a security incident, the IT Operation Department **MUST** initiate the appropriate countermeasures (see also *DER.2.1 Security Incident Handling*):

- At the point where the WLAN communication enters the internal LAN, communications **SHOULD** be blocked selectively for every SSID and access point, or even for the entire WLAN infrastructure, in the event of an attack.
- If access points have been stolen, defined security safeguards **MUST** be implemented to prevent any misuse of the access points.
- If WLAN clients have been stolen and central certificate-based authentication is being used, the client certificates **MUST** be blocked.

The possible consequences of events critical to security **MUST** be examined. Ultimately, the possibility of using stolen devices without authorisation in order to access the network of the organisation **MUST** be ruled out.

Standard Requirements

For module NET.2.1 *WLAN Operation*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

NET.2.1.A9 Secure Connection of WLANs to a LAN [Planner]

If WLANs are connected to a LAN, the transition between WLANs and the LAN **SHOULD** be protected – for example, with the help of a packet filter. The access point **SHOULD** be integrated in line with the requirements of NET.2.1.A7 *Setting Up a Distribution System*.

NET.2.1.A10 Drawing Up a Security Policy for WLAN Operation

Based on the general security policy of the organisation, the essential core aspects **SHOULD** be specified for the secure use of WLANs. The policy **SHOULD** be known to all persons in charge who are involved in establishing and operating WLANs and must form the foundation of their work. The implementation of the contents required in the policy **SHOULD** be checked at regular intervals. The results **SHOULD** be documented in an appropriate manner.

NET.2.1.A11 Selection of Suitable WLAN Components

If the decision to establish a WLAN infrastructure has been made, the results of the planning phase **SHOULD** be used to create a requirements list that can be used to evaluate the products available on the market. When procuring WLAN components, data protection and the inter-compatibility of the WLAN components **SHOULD** be taken into account along with security.

NET.2.1.A12 Use of a Suitable WLAN Management Solution

In order to be able to guarantee an ideal configuration of the WLAN components from a security point of view, a central management solution **SHOULD** be used. The functional range of the solution used **SHOULD** be in accordance with the requirements of the WLAN strategy.

NET.2.1.A13 Regular Security Checks of WLANs

WLANs **SHOULD** be checked regularly as to whether there might be vulnerabilities. In addition, the WLANs provided **SHOULD** be searched for access points that have been installed without authorisation. Furthermore, the performance **SHOULD** be measured. The results of security checks **SHOULD** be documented transparently and compared against the target condition. Deviations **SHOULD** be investigated.

NET.2.1.A14 Regular Audits of WLAN Components

All components of the WLAN infrastructure (access points, distribution system, WLAN management solution, etc) **SHOULD** be checked regularly as to whether all the defined security safeguards have been implemented and whether these components are configured correctly. Publicly mounted access points **SHOULD** be checked randomly at regular intervals as to whether there have been attempts to open or manipulate them by force. The audit results **SHOULD** be documented transparently and compared against the target condition. Deviations **SHOULD** be investigated.

Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.2.1 *WLAN Operation* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

NET.2.1.A15 Using a VPN to Secure WLANs (CI)

In the event of increased protection needs, a VPN SHOULD be used for added protection of communications via the WLAN infrastructure. Additional information on this can be found in module NET.3.3 *VPN*.

NET.2.1.A16 Additional Protection When Connecting WLANs to a LAN (CIA)

If a WLAN infrastructure is connected to a LAN, the transition between WLANs and the LAN SHOULD have added protection in line with increased protection needs.

NET.2.1.A17 Protecting Communication Between Access Points (C)

Communications between the access points that take place via the radio interface and the LAN SHOULD be encrypted in order to ensure the confidentiality of the data transmitted (e.g. roaming information or access data of users).

NET.2.1.A18 Use of Wireless Intrusion Detection / Wireless Intrusion Prevention Systems (CIA)

In order to be able to promptly detect security incidents and vulnerabilities and immediately initiate corresponding countermeasures, wireless intrusion detection systems and wireless intrusion prevention systems SHOULD be used.

Additional Information

For more information about threats and security safeguards for module NET.2.1 *WLAN Operation*, see the following publications, among others:

[BSIDKS]	Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte [Wireless Communication Systems and their Security Aspects]: Federal Office for Information Security (BSI), 2009, https://www.bsi.bund.de/DE/Publikationen/Broschueren/Drahtloskom/drahtloskom.html , last accessed on 05.10.2018
[ISIWLAN]	BSI Standard on Internet Security (ISi series): Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA) [Secure connection of local networks to the Internet (Isi-LANA)], Federal Office for Information Security (BSI), 2014, last accessed on 05.10.2018 https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html
[NIST800153]	Guidelines for Securing Wireless Local Area Network (WLANs): NIST Special Publication 800-153, February 2013, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf , last accessed on 05.10.2018
[NIST80097]	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11, NIST Special

	Publication 800-97, February 2007, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nist-specialpublication800-97.pdf , last accessed on 05.10.2018
[TR03103]	Technical Guidelines Secure Wireless LAN: Federal Office for Information Security (BSI), October 2005, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03103/index_hm.html , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.2.1 *WLAN Operation*:

- G 0.9 Failure or Disruption of Communication Networks
- G 0.15 Eavesdropping
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.23 Unauthorised Access to IT Systems
- G 0.24 Destruction of Devices or Storage Media
- G 0.25 Failure of Devices or Systems
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.40 Denial of Service
- G 0.43 Attack with Specially Crafted Messages
- G 0.44 Unauthorised Entry to Premises

Elementary Threats Requirements	G 0.9	G 0.15	G 0.16	G 0.18	G 0.23	G 0.24	G 0.25	G 0.30	G 0.31	G 0.40	G 0.43	G 0.44
NET.2.1.A1				X								
NET.2.1.A2	X	X		X	X			X			X	
NET.2.1.A3		X		X	X			X			X	
NET.2.1.A4	X		X	X		X	X			X		X
NET.2.1.A5		X			X			X	X		X	
NET.2.1.A6		X			X			X	X		X	
NET.2.1.A7		X		X	X							
NET.2.1.A8		X										
NET.2.1.A9		X		X	X				X			
NET.2.1.A10		X		X								
NET.2.1.A11				X								
NET.2.1.A12			X		X		X	X	X	X	X	
NET.2.1.A13					X			X		X	X	
NET.2.1.A14					X			X		X	X	
NET.2.1.A15		X			X			X	X		X	
NET.2.1.A16		X			X			X				
NET.2.1.A17		X			X							
NET.2.1.A18					X			X		X	X	



NET.2.2: WLAN Usage

Description

Introduction

Wireless LANs (WLANs) can be used to create wireless local networks or extend existing wired networks. Up to now, almost all WLAN components available on the market have been based on the IEEE 802.11 standard and its additions. The Wi-Fi Alliance, a consortium of companies, plays an important role in this regard as the creator of the industry-agreed “Wi-Fi” standard based on IEEE 802.11. The Wi-Fi Alliance uses the Wi-Fi quality label to confirm that a device has passed certain interoperability and conformity tests.

WLANs provide added convenience and mobility, but their use also poses an additional potential threat to information security because the communication is wireless. That is why it is absolutely necessary that both the persons in charge of IT and the users be aware of possible risks that may occur if WLANs are used improperly. This means that the users must have the required knowledge to correctly understand and apply security safeguards. In particular, they must know what is expected of them in terms of information security and how they should respond in certain situations when using WLANs.

Objective

This module is designed to show how WLANs can be used in a secure manner.

Not in Scope

The module includes basic requirements to be considered and fulfilled when using WLANs in order to be able to counteract the specific threats. Requirements for the secure operation of WLANs are not included in the present module; they are described in module NET.2.1 *WLAN Operation*. Moreover, the module does not deal with general aspects of a client. Such aspects are described in module SYS.2.1 *General Client*.

Threat Landscape

For module NET.2.2 *WLAN Usage*, the following specific threats and vulnerabilities are of particular importance:

Insufficient Knowledge of Rules and Procedures

If the users are not adequately familiar with the rules for the proper handling of WLANs, they will not be able to adhere to them. For example, if WLAN clients are connected carelessly to external networks, the information transmitted (e.g. session cookies, passwords) can be intercepted.

Non-Compliance with Security Measures

Due to negligence and insufficient checks, it is relatively common for people to fail to consider some or all of the security measures that have been recommended to them or that they are required to implement. For example, if a WLAN client is used in ad-hoc mode although this is expressly prohibited in the user policy, another client may communicate directly with the WLAN client and (for example) access confidential documents stored on the client without authorisation.

Eavesdropping on WLAN Communication

Since radio is a medium that can be shared by several users, the data transmitted via WLANs can easily be intercepted and recorded. If the data is insufficiently encrypted (or not at all), transmitted payload data can easily be obtained. Furthermore, wireless networks and the radio waves emitted often radiate beyond the rooms in which the networks are used, making it possible for data to be sent to areas which cannot be controlled and secured by the users or an organisation.

Analysis of Connection Data Related to Wireless Communication

In WLANs based on IEEE 802.11, the MAC address of a WLAN card is sent every time data is transmitted. Since this transmission is not encrypted, movement profiles can be created for mobile users – for example, when and where the users log into public hotspots.

Simulating a Valid Access Point (Rogue Access Points)

An attacker can masquerade as a part of the WLAN infrastructure by installing their own access point with a suitable SSID in the vicinity of a client. A simulated access point of this kind is referred to as a “rogue access point”. If this access point provides the WLAN client with stronger transmission performance than the real access point, the client will use it as its base station if mutual authentication is not enforced. Furthermore, the real access point may be disabled by a denial-of-service attack. The users log into a network that only pretends to be the target network. This makes it possible for an attacker to eavesdrop on communications. Poisoning or spoofing methods can also simulate a false identity for an attacker or redirect the network traffic to the attacker's systems. This means that the attacker can listen in on and control communications. Particularly in public radio networks (hotspots), a rogue access point is a frequently used means of attack.

Requirements

The specific requirements of module NET.2.2 *WLAN Usage* are listed below. As a matter of principle, the user is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	User
Further Roles	IT Operation Department, Head of IT, Super-

	visor
--	-------

Basic Requirements

For module NET.2.2 *WLAN Usage*, the following requirements **MUST** be implemented as a matter of priority:

NET.2.2.A1 Creating a User Policy for WLAN [Head of IT]

The essential core aspects of secure WLAN usage **MUST** be specified in a WLAN usage policy based on the general security policy of the organisation. This user policy **MUST** describe the particularities of WLAN usage (e.g. whether and how hotspots may be used).

Furthermore, the policy **MUST** contain specifications (especially for the use of classified information) regarding which data is used in the WLAN and which data may and may not be transmitted over the WLAN.

It **MUST** describe how to handle client-side security solutions. The user policy **MUST** contain a clearly stated ban on connecting unauthorised access points to the LAN of the organisation. Moreover, the policy **MUST** state that the WLAN interface **MUST** be deactivated if it is not used for a longer period.

It **MUST** be checked regularly that the contents required in the policy have been implemented correctly. The results **SHOULD** be documented in an appropriate manner.

NET.2.2.A2 Awareness and Training of WLAN Users [Supervisor, Head of IT]

The users of WLAN components (mainly of WLAN clients) **MUST** be made aware of and trained on the safeguards stated in the user policy. The meanings of the WLAN-specific security settings and why they are important **MUST** be explained in detail to the users. In addition, they **MUST** be informed of the threats that result from bypassing or disabling these security settings.

The contents of the training program **MUST** always be adapted to the corresponding operational scenarios. In addition to receiving training on WLAN security mechanisms, the users **MUST** be given a copy of the WLAN security policy of the organisation. Furthermore, they **MUST** be made aware of the risks when they are required to use external WLANs.

NET.2.2.A3 Safeguarding WLAN Usage in Insecure Environments [IT Operation Department]

If external hotspots **MAY** be used, the following **MUST** be implemented:

- Every hotspot user **MUST** know their security requirements (see NET.2.2.A2 *Awareness and Training of WLAN Users*) and then decide if or under which conditions hotspot use is allowed.
- The users **SHOULD** delete any sporadically used WLANs from their history.
- If possible, separate user accounts with a secure basic configuration and restrictive authorisations **SHOULD** be used.

- It SHOULD be ensured that a user with administrator rights can never log into external WLANs from their client.
- Sensitive data MAY ONLY be transmitted if appropriate security safeguards are implemented and secure protocols are used.
- When using publicly available WLANs, the users MAY ONLY access internal resources of the organisation via a virtual private network (VPN). Additional information on this can be found in module NET.3.3 VPN.

Standard Requirements

For module NET.2.2 *WLAN Usage*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

NET.2.2.A4 Procedures in the Event of WLAN Security Incidents

In case of WLAN security incidents, the users SHOULD perform the following:

- They SHOULD save the results of their work, terminate the WLAN connection and disable the WLAN interface of their client.
- The users SHOULD document any error messages and abnormalities as precisely as possible. The users SHOULD also document what they were doing before and during the security incident.
- The IT Operation Department MUST be informed by the users using a suitable escalation level (e.g. a user help desk).

Requirements in Case of Increased Protection Needs

For module NET.2.2 *WLAN Usage* there are no Requirements in Case of Increased Protection Needs.

Additional Information

For more information about threats and security safeguards for module NET.2.2 *WLAN Usage*, see the following publications, among others:

[BSIDKS]	Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte [Wireless Communication Systems and their Security Aspects]: Federal Office for Information Security (BSI), 2009, https://www.bsi.bund.de/DE/Publikationen/Broschueren/Drahtloskom/drahtloskom.html , last accessed on 05.10.2018
[ISILANA]	Secure Connection of Local Networks to the Internet (ISi-LANA): Federal Office for Information Security (BSI), Version 2.1, August 2014 https://www.bsi.bund.de/DE/The-men/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html , last accessed on 05.10.2018
[NIST800153]	Guidelines for Securing Wireless Local Area Network (WLANs): NIST Special Publication 800-153, February 2013, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspe-

	cialpublication800-153.pdf , last accessed on 05.10.2018
[NIST80097]	Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11, NIST Special Publication 800-97, February 2007, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nist-specialpublication800-97.pdf , last accessed on 05.10.2018
[TR03103]	Technical Guidelines Secure Wireless LAN: Federal Office for Information Security (BSI), October 2005, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03103/index_htm.html , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.2.2 *WLAN Usage*:

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.23 Unauthorised Access to IT Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.43 Attack with Specially Crafted Messages

Elementary Threats Requirements	G 0.15	G 0.18	G 0.23	G 0.31	G 0.43
NET.2.2.A1	X	X	X	X	X
NET.2.2.A2	X	X	X	X	X
NET.2.2.A3	X		X		X
NET.2.2.A4			X		



NET.3.1: Routers and Switches

Description

Introduction

Routers and switches form the backbone of today's IT networks. The failure of one or more of these devices may lead to the complete standstill of the entire IT infrastructure. Therefore, they require special protection.

Routers work on OSI layer 3 (the network layer) and transport data packets based on the destination IP address in the IP header. Routers are able to connect networks with different topologies. They are used to segment local networks or connect local networks via wide area networks. A router identifies a suitable connection between the source system or network and the destination system or network. In most cases, this is performed by forwarding the data packets to the next router.

Initially, switches worked on OSI layer 2, but switches with different functions are now available. Manufacturers usually identify the devices according to the OSI layer they support. This has resulted in the terms layer 2, layer 3, and layer 4 switch, whereby layer 3 and layer 4 switches are actually already routers in functional terms. Today, the initially different functions of switches and routers are thus frequently combined in one device.

Objective

This module describes the secure operation of routers and switches.

Not in Scope

A huge selection of different routers and switches from different manufacturers are available on the market. The module does not describe any specific requirements for certain products. It is designed to be as manufacturer-agnostic as possible.

Due to the amalgamation of the functions of routers and switches, the majority of the requirements are applicable to both routers and switches. In most instances, the present module does not differentiate between these device types.

Today, nearly all operating systems also offer a routing feature. This module does not mention any requirements for enabled routing features in operating systems.

Furthermore, aspects of infrastructural security (e.g. appropriate installation, or power supply or cabling) are not discussed in this module; they can be found in the respective modules of the layer INF *Infrastructure*.

The present module does not describe any requirements regarding how virtual routers and switches can be secured. Security aspects of virtual active network components are addressed in module NET.1.4 *Network Virtualisation*. The firewall features that routers and switches may offer are not addressed either. Module NET.3.2 *Firewall* must be implemented in this regard. Some aspects of network design and management are also important for using routers and switches and will be mentioned within the framework of the corresponding requirements. Additional information for establishing, designing and managing a network can be found in the modules NET.1.1 *Network Architecture and Design* and NET.1.2 *Network Management*.

Threat Landscape

For module NET.3.1 *Routers and Switches*, the following specific threats and vulnerabilities are of particular importance:

Distributed Denial of Service (DDoS)

Within the framework of a DDoS attack on a protected network (for example, via TCP-SYN flooding or a UDP packet storm), the large number of network connections that must be processed may result in the router failing. This may render certain services unavailable in the local area network (LAN) or cause the entire LAN to fail.

Manipulation

If an attacker manages to access a router or switch without authorisation, they might re-configure the devices or even start additional services. For example, the configuration may be changed in a way that blocks services, clients or entire network segments.

Software Vulnerabilities or Errors

Manufacturers of routers and switches regularly publish updates and patches designed to eliminate software errors and vulnerabilities that have come to light in their products. However, if these are installed too late (or not at all), the router or switch may be attacked successfully. As a consequence, it may be possible for attackers to manipulate the systems so that business-critical data leaks, services fail or entire production processes come to a standstill.

Incorrect Configuration of a Router or Switch

Routers and switches are delivered with a default configuration in which many services are activated. Login banners also give away the model and version numbers of the device, for example. When routers and switches with insecure factory settings are used in production environments, it is easier to access them without authorisation. This may render services unavailable, for example.

Improper Planning and Design

Many organisations plan and design the use of routers and switches improperly. Among other things, this results in devices being procured that are not dimensioned sufficiently (in terms of performance or the number of ports, for example). As a consequence, the router or switch is already overloaded the first time it is used. This means that services or entire networks might not be available and considerable resources may be required to correct the error.

Incompatible Active Network Components

Compatibility issues may occur, particularly if existing networks are complemented by active network components of other manufacturers or networks are operated with components of different manufacturers. If active network components with different implementations of the same communication method are operated together in one and the same network, individual sub-areas of the network, of certain services, or even the entire network may fail.

MAC Flooding

During MAC flooding, an attacker sends a large amount of requests with different source MAC addresses to a switch. Once the switch has reached the maximum number of MAC addresses it can store, it starts sending all requests to all IT systems in the network. As a consequence, the attacker may view the network traffic.

Spanning Tree Attacks

During spanning tree attacks, an attacker sends so-called Bridge Protocol Data Units (BPDUs) in order to induce the switches to consider their own (malicious) switch as the root bridge. The network traffic is thereby routed through the switch of the attacker, enabling them to record all information sent using this switch. As a consequence, the attacker might initiate DDoS attacks and force the network to re-establish the spanning tree topology with the help of incorrect BPDUs, which might cause the network to fail.

GARP Attacks

During gratuitous ARP (GARP) attacks, the attacker sends unrequested ARP replies to certain targets or to all the IT systems in the same sub-network. In this forged ARP reply, the attacker enters their MAC address as an assignment to a third-party IP address and induces the target to change their ARP table in such a way that the network traffic will then be sent to the attacker instead of the valid destination. As a consequence, the attacker may record or manipulate the communication between the targets.

Requirements

The specific requirements of module NET.3.1 *Routers and Switches* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept defined. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO)

Basic Requirements

For module NET.3.1 *Routers and Switches*, the following requirements **MUST** be implemented as a matter of priority:

NET.3.1.A1 Secure Basic Configuration of a Router or Switch

Prior to using a router or switch, it MUST be configured securely. The devices MUST ONLY be installed and configured by persons authorised to do so. All changes to the configuration SHOULD be documented transparently (see NET.3.1.A9 *Operational Documentation*). The integrity of the configuration files MUST be protected appropriately. Access passwords MUST be stored in an encrypted form.

Routers and switches MUST be configured in such a way that only absolutely necessary services, protocols and functional extensions are used. Services, protocols and functional extensions that are not required MUST be disabled or uninstalled completely. Unused interfaces on routers and switches MUST also be disabled. If possible, unused network ports MUST be disabled or at least assigned to an *unassigned VLAN* set up for this purpose.

If functional extensions are used, the security policies of the organisation MUST continue to be met. It SHOULD also be justified and documented why such extensions are used.

Information on the internal configuration and operating status MUST be hidden from third parties. Unnecessary information services MUST be disabled.

Prior to commissioning routers and switches, the default user accounts MUST be changed. The passwords of these accounts MUST be changed. Unused user accounts MUST be deactivated. After that, the planned user accounts and roles MUST be configured according to the access control policy and role concept.

NET.3.1.A2 Installing Updates and Patches

The persons in charge MUST obtain information on known vulnerabilities. Updates and patches MUST be installed as quickly as possible. Before this occurs, a test system SHOULD be used to check whether the security updates are compatible and do not cause any errors. As long as no patches are available for known vulnerabilities, other appropriate safeguards MUST be implemented in order to protect routers and switches.

It MUST be ensured that patches and updates are only obtained from trustworthy sources. If offered by the manufacturer, the update checksums SHOULD be compared and the digital signatures SHOULD be checked.

NET.3.1.A3 Restrictive Granting of Access Rights

It MUST be specified who may access a router or switch. In so doing, ONLY the access rights necessary to perform the corresponding tasks MAY be granted (minimum principle). User accounts no longer needed MUST be deleted. It MUST be ensured that administrator rights (and root rights) are only used when this is necessary.

NET.3.1.A4 Protection of Administration Interfaces

All administration and management access to routers and switches MUST be restricted to individual source IP addresses or address ranges. It MUST be ensured that it is not possible to access the administration interfaces directly from untrusted networks.

In order to administer and monitor routers and switches, sufficiently encrypted protocols SHOULD be used. If non-encrypted (and thereby insecure) protocols are nevertheless used, a separate administration network (out-of-band management) MUST be used for the administrators. The management interfaces and administration connections MUST be protected by means of a separate firewall. Appropriate time limits MUST be specified for the interfaces.

All services not required for the management interface **MUST** be disabled. If a network component has a dedicated hardware interface, any unauthorised access to this interface **MUST** be prevented appropriately.

NET.3.1.A5 Protection Against Fragmentation Attacks

Protection mechanisms **MUST** be enabled on the router and the layer 3 switch in order to fend off IPv4 and IPv6 fragmentation attacks.

NET.3.1.A6 Emergency Access to Routers and Switches

The administrators **MUST** always be capable of directly accessing routers and switches to ensure continuous administration even if the entire network fails.

NET.3.1.A7 Logging on Routers and Switches

A router or switch **MUST** be configured in such a way that it logs the following events, among others:

- configuration changes (automatically whenever possible)
- reboots
- system errors
- status changes on each interface, system and network segment
- login errors (at least if they occur more than once)

The persons in charge **MUST** ensure that all legal framework conditions are complied with during logging. Changes to the configuration **SHOULD** also be logged automatically.

NET.3.1.A8 Regular Backups

The configuration files of routers and switches **MUST** be backed up at regular intervals. The backup copies **MUST** be created in such a way that they can be accessed in an emergency.

NET.3.1.A9 Operational Documentation

The most important operational tasks of a router or switch **MUST** be documented appropriately. All configuration changes and security-relevant tasks **SHOULD** be documented. The documentation **SHOULD** be protected against unauthorised access.

Standard Requirements

For module NET.3.1 *Routers and Switches*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

NET.3.1.A10 Drawing Up a Security Policy [Chief Information Security Officer (CISO)]

Based on the general security policy of the organisation, a specific security policy **SHOULD** be drawn up that transparently describes the requirements and specifications of secure router and switch operations. The policy **SHOULD** be known to all administrators and **SHOULD** be the basis of their work. If the policy is changed or deviations from the requirements are allowed, this **SHOULD** be coordinated with the CISO and documented. It **SHOULD** be checked regularly

whether the policy is still implemented properly. The results SHOULD be documented appropriately.

NET.3.1.A11 Procurement of a Router or Switch

Prior to procuring routers and switches, a requirements list SHOULD be drawn up that can be used to evaluate the products available on the market. It SHOULD be ensured that the desired security level of the organisation can be achieved with the devices to be procured. The procurement process SHOULD thus be based on the requirements from the security policy.

NET.3.1.A12 Drawing Up a Configuration Checklist for Routers and Switches

A configuration checklist SHOULD be created that can be used to check the most important security-relevant settings on routers and switches. Since the secure configuration strongly depends on the purpose at hand, the different requirements of the devices SHOULD be taken into consideration within the framework of the configuration checklist.

NET.3.1.A13 Administration Using a Separate Management Network

Routers and switches SHOULD only be administered using a separate management network (out-of-band management). If one exists, the administration interface via the actual data network (in-band) SHOULD be disabled. The available security mechanisms of the management protocols used for authentication, integrity protection and encryption SHOULD be enabled and all insecure management protocols SHOULD be disabled (see NET.1.2 *Network Management*).

NET.3.1.A14 Protection Against Misuse of ICMP Messages

It SHOULD be ensured that the protocols ICMP and ICMPv6 are filtered restrictively.

NET.3.1.A15 Bogon and Spoofing Filtering

Attackers SHOULD be prevented from entering the routers and switches with the help of forged, reserved or unassigned IP addresses.

NET.3.1.A16 Protection Against IPv6 Routing Header Type-0 Attacks

When using IPv6, mechanisms SHOULD be used to detect and prevent attacks on the type-0 routing header.

NET.3.1.A17 Protection Against DoS and DDoS Attacks

Mechanisms SHOULD be used that detect and fend off high-volume attacks and TCP state exhaustion attacks.

NET.3.1.A18 Configuration of Access Control Lists

Access to routers and switches SHOULD be defined with the help of access control lists (ACL). Based on the security policy of the organisation, the ACL SHOULD define which IT systems or networks (and corresponding methods) may be used to access a router or switch. If there are no specific rules, the restrictive whitelist approach SHOULD be preferred as a matter of principle.

NET.3.1.A19 Protection of Switch Ports

The ports of a switch SHOULD be protected against unauthorised access.

NET.3.1.A20 Security Aspects of Routing Protocols

Routers SHOULD authenticate themselves when exchanging routing information or transmitting updates for routing tables. Only routing protocols that support this SHOULD be used.

Dynamic routing protocols SHOULD only be used in secure networks. They MUST NOT be used in demilitarised zones (DMZ). Static routes SHOULD be entered instead in DMZs.

NET.3.1.A21 Identity and Authorisation Management in the Network Infrastructure

Routers and switches SHOULD be connected to a central identity and authorisation management system (see ORP.4 *Identity and Access Management*).

NET.3.1.A22 Contingency Planning for Routers and Switches

In order to be able to react quickly and effectively when disruptions occur, diagnostics and troubleshooting SHOULD be planned and prepared in advance. Corresponding instructions SHOULD be defined for typical failure scenarios.

The contingency planning for routers and switches SHOULD be coordinated with the overall failure and contingency planning concept (see DER.4 *Business Continuity Management*). It SHOULD be ensured that the contingency planning documentation and the instructions contained therein exist in paper form. The described approaches required in the field of contingency planning SHOULD be drilled and practised at regular intervals.

NET.3.1.A23 Audits and Penetration Tests

Routers and switches SHOULD be checked for known security issues at regular intervals. Audits SHOULD also be performed regularly. This SHOULD include checks as to whether the actual situation corresponds to the secure basic configuration defined. The results SHOULD be clearly documented and compared against the target situation. Deviations SHOULD be investigated.

Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.3.1 *Routers and Switches* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

NET.3.1.A24 Use of Network Access Controls (IA)

Port-based access control according to IEEE 802.1x SHOULD be implemented on the basis of EAP-TLS. Implementations according to the standards IEEE 802.1x-2001 and IEEE 802.1x-2004 SHOULD NOT be performed.

NET.3.1.A25 Advanced Integrity Protection for Configuration Files (I)

If a router or switch crashes, it SHOULD be ensured that no legacy or incorrect configurations (among other things, ACLS) are used during recovery and restart.

NET.3.1.A26 High Availability (A)

The implementation of a high-availability solution MUST NOT impair the operation of the routers and switches or their security features, or reduce the level of security. Routers and

switches SHOULD be designed redundantly. In so doing, it SHOULD be ensured that the security policy of the organisation is observed.

NET.3.1.A27 Bandwidth Management for Critical Applications and Services (A)

In order to guarantee bandwidth management for critical applications and services, routers and switches SHOULD include and use features that can be used to identify applications and prioritise bandwidth.

NET.3.1.A28 Use of Certified Products (CI)

Routers and switches with a Common Criteria security evaluation of at least EAL4 SHOULD be used.

Additional Information

For more information about threats and security safeguards for module NET.3.1 *Routers and Switches*, see the following publications, among others:

[8021AE]	IEEE 802.1AE-2018: IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security, December 2018, https://standards.ieee.org/standard/802_1AE-2018.html , last accessed on 05.10.2018
[8021Q]	IEEE 802.1Q-2014: (Revision of IEEE Std. 802.1Q-2011), IEEE Standard for Local and Metropolitan Area Networks - Bridges and Bridged Networks, 2014, http://standards.ieee.org/findstds/standard/802.1Q-2014.html , last accessed on 15.11.2017
[ISI]	BSI Standards on Internet Security (ISi series): https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-Reihe_node.html , last accessed on 05.10.2018
[NIST80046]	Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security: NIST Special Publication 800-46, Revision 2, July 2016, http://dx.doi.org/10.6028/NIST.SP.800-46r2 , last accessed on 05.10.2018
[RFC6165]	Extensions to IS-IS for Layer-2 Systems: RFC 6165, April 2011, https://tools.ietf.org/html/rfc6165 , last accessed on 05.10.2018
[RFC7348]	Virtual EXTensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks, RFC 7348, August 2014, https://tools.ietf.org/html/rfc7348 , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.3.1 *Routers and Switches*:

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.29 Violation of Laws or Regulations

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.36 Identity Theft

G 0.37 Repudiation of Actions

G 0.38 Misuse of Personal Information

G 0.40 Denial of Service

G 0.42 Social Engineering

G 0.43 Attack with Specially Crafted Messages

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	0.9	0.1	0.4	0.5	0.6	0.7	0.8	0.9	0.0	0.1	0.2	0.3	0.5	0.6	0.7	0.8	0.9	0.0	0.1	0.2	0.6	0.7	0.8	0.0	0.2	0.3	0.5	0.6	
NET.3.1.A1	X				X	X	X	X		X	X			X															
NET.3.1.A2		X	X	X									X	X				X	X	X	X			X		X			
NET.3.1.A3			X	X									X																
NET.3.1.A4	X	X	X	X								X						X	X	X	X		X						
NET.3.1.A5	X		X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X		X	X	X
NET.3.1.A6			X	X										X									X						
NET.3.1.A7		X																											
NET.3.1.A8		X																					X						
NET.3.1.A9	X	X	X	X																									
NET.3.1.A10												X																	
NET.3.1.A11	X	X	X	X								X						X	X	X	X		X						
NET.3.1.A12	X	X	X	X								X						X	X	X	X	X	X	X					
NET.3.1.A13	X		X	X			X	X				X	X	X	X	X	X	X	X	X	X	X		X					



NET.3.2: Firewall

Description

Introduction

A firewall is a system consisting of hardware and software components that is used to securely connect IP-based data networks. It uses a firewall structure to restrict the communication that is technically feasible to what is defined as secure in a security policy. In this context, security means that only the access or data streams desired between different networks are allowed.

In many cases, securing network gateways no longer involves an individual component; a whole range of IT systems takes on different tasks (e.g. filtering packets exclusively or strictly disconnecting network connections with the help of proxy features). The term "application level gateway" (ALG), which is used in this module, refers to a firewall component that controls data streams on the basis of security proxies.

A firewall is installed at the main gateway between networks with differing levels of trustworthiness. Internet-to-intranet connections are not the only example of networks with different levels of trustworthiness. An organisation may have two internal networks with different protection needs: for instance, the protection needs of the office communication network frequently differ from those of the human resources department network, which transmits personal data that is particularly sensitive.

Objective

The objective of this module is to ensure the ability make secure use of a firewall or a firewall structure in order to securely connect networks with different protection needs.

Not in Scope

The present module builds upon module NET.1.1 *Network Architecture and Design* and includes specific requirements to be observed and complied with when procuring, establishing, configuring and operating network-based firewalls.

In order to secure networks, additional network components are typically required (e.g. routers and switches). The related requirements are not covered in this module, but can be found in NET.3.1 *Routers and Switches*. If a firewall assumes the tasks of a router or switch, the requirements included in module NET.3.1 *Routers and switches* also apply to the firewall.

Furthermore, products such as "next-generation" firewalls (NGFW) or unified threat management firewalls that also include functional extensions are not addressed (e.g. VPN, intrusion detection and intrusion prevention systems (IDS/IPS), virus scanners or spam filters). Security aspects of these functional extensions are not part of the present module; they are addressed in

the modules NET.3.3 *VPN*, NET.3.4 *IDS/IPS* and OPS1.1.4 *Protection Against Malware*, for example.

Application detection and filtering are not addressed either. These are common features of next-generation firewalls and IDS/IPS. Since these products involve different implementations, it is advisable to consider them individually depending on the use scenario. This module does not address the individual protection options for server services that are offered externally, such as through a reverse proxy or for web services with the help of a web application firewall (WAF). Furthermore, aspects of infrastructural security (e.g. appropriate installation or power supply) are not discussed in this module; they can be found in the respective modules of the INF layer.

Threat Landscape

For module NET.3.2 *Firewall*, the following specific threats and vulnerabilities are of particular importance:

Distributed Denial of Service (DDoS)

Within the framework of a DDoS attack on a protected network (e.g. via TCP-SYN flooding or a UDP packet storm), the large number of network connections that must be processed may result in the firewall failing. This may render certain services unavailable in the local area network (LAN) or cause the entire LAN to fail.

Manipulation

If an attacker manages to access a firewall system or a corresponding administration interface, they may manipulate data in any number of ways. For example, they may change the configuration, start additional services or install malware. They may also tap the communication links on the manipulated system. For example, the firewall rules may be changed in such a way that it is possible to access the firewall and the intranet of the organisation from the Internet. Furthermore, an attacker may start a denial-of-service attack (DoS) by preventing access to individual server services in the rule set.

Software Vulnerabilities or Errors

Firewalls are complex systems that are exposed to numerous attacks, specifically at the gateway between the intranet and the Internet. Hence, manufacturers of firewalls regularly publish updates and patches designed to eliminate software errors and vulnerabilities that have come to light in their products. However, if these are too late (or not at all), the firewall system may be attacked successfully. As a consequence, it may be possible for attackers to manipulate the systems so that business-critical data leaks, services fail or entire production processes come to a standstill.

Bypassing Firewall Rules

Attackers may use basic mechanisms in the network protocols to bypass the firewall rules (e.g. through fragmentation attacks) and enter an area protected by the firewall. In the protected area, they may then cause additional damage (e.g. by accessing, manipulating, or deleting sensitive data).

Incorrect Configuration and Errors in Operating a Firewall

An improperly configured or operated firewall may have dramatic effects on the availability of services. If, for example, firewall rules are set improperly, network access may be blocked. Furthermore, incorrect configurations may result in insufficient protection of IT systems (or none at all). In the worst-case scenario, this might make internal services accessible for attackers.

Requirements

The specific requirements of module NET.3.2 *Firewall* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO)

Basic Requirements

For module NET.3.2 *Firewall*, the following requirements **MUST** be implemented as a matter of priority:

NET.3.2.A1 Drawing Up a Security Policy [Chief Information Security Officer (CISO)] (I)

Based on the general security policy of the organisation, a specific security policy **MUST** be drawn up that transparently describes requirements and specifications for secure firewall operation. The policy **MUST** be known to all employees in charge in the field of firewalls and **MUST** be the basis of their work. If the policy is changed or deviations from the requirements are allowed, this **MUST** be agreed with the CISO and documented. The correct implementation of the policy **MUST** be regularly reviewed. The results **MUST** be documented in an appropriate manner.

NET.3.2.A2 Definition of Firewall Rules

All communications between the participating networks **MUST** go through the firewall. It **MUST** be ensured that no unauthorised connections from the outside can be established into the protected network. In addition, unauthorised connections **MUST NOT** be established from the protected network.

Unambiguous rules **MUST** be defined for the firewall that specify which communication links and data streams are allowed. Any other connections **MUST** be prevented by the firewall (whitelist approach). The communication relationships with connected service servers (e.g. e-mail servers, web servers) that are routed through the firewall **MUST** be taken into consideration in the rules.

IT systems **MUST NOT** be allowed to access the internal network via the firewall from the outside (see specifications from module NET.1.1 *Network Architecture and Design*). Possible excep-

tions to this requirement are specified in the corresponding application- and system-specific modules.

Persons in charge **MUST** be appointed to develop, implement and test filter rules. Additionally, it **MUST** be clarified who may change filter rules. The decisions taken and the relevant information and reasons for them **MUST** be documented.

NET.3.2.A3 Configuring Appropriate Filter Rules on the Packet Filter

Based on the firewall rules from NET.3.2.A2 *Definition of Firewall Rules*, appropriate filter rules must be defined and configured for the packet filter.

A packet filter **MUST** be configured in such a way that it discards any invalid TCP flag combinations. As a matter of principle, filtering **MUST** always be performed in a stateful manner. Stateful filter rules **SHOULD** also be configured for the protocols without any connection (UDP and ICMP). The firewall **MUST** filter the ICMP and ICMPv6 protocols restrictively.

NET.3.2.A4 Secure Firewall Configuration

Before a firewall is used, it **MUST** be configured securely.

A firewall **MAY ONLY** be installed and configured by persons authorised to do so, such as those in charge from the internal IT Operation Department or contractually bound service providers.

All changes to the configuration **MUST** be documented transparently (see NET.3.2.A14 *Operational Documentation*). The integrity of the configuration files **SHOULD** be protected appropriately. Access passwords **MUST** be stored in an encrypted form.

A firewall **MUST** be configured in such a way that only absolutely required services are available. If functional extensions are used, the security policies of the organisation **MUST** continue to be met. It **MUST** also be justified and documented why such extensions are used. Any unnecessary (information) services and functional extensions **MUST** be disabled or uninstalled completely.

Information on the internal configuration and operating status **MUST** be hidden from third parties whenever possible.

NET.3.2.A5 Restrictive Granting of Access Rights

It **MUST** be specified who may access the firewall (e.g. in order to configure or monitor the firewall). In so doing, the access rights granted to perform the corresponding tasks **MUST** be kept to the necessary minimum (“need-to-know” principle). Unauthorised user accounts **MUST** be deleted. It **MUST** be ensured that administrator rights (and root rights) are only used when this is necessary.

NET.3.2.A6 Protection of Administration Interfaces

All administration and management access to the firewall **MUST** be restricted to individual source IP addresses or address ranges. It **MUST** be ensured that it is not possible to access the administration interfaces from non-trustworthy networks.

In order to administer and monitor the firewall, secure protocols or a dedicated administration network (out-of-band management) **MUST** be used (see specifications from the modules

NET.1.1 *Network Architecture and Design* and NET.1.2 *Network Management*). Appropriate time limits MUST be specified for the user interfaces.

NET.3.2.A7 Emergency Access to the Firewall

It MUST always be possible to access the firewall directly so that it is always possible to work locally, even if the entire network has failed.

NET.3.2.A8 Prevention of Dynamic Routing

Dynamic routing MUST be disabled in the settings of the firewall unless the packet filter is used as a perimeter router in accordance with module NET.3.1 *Routers and Switches*.

NET.3.2.A9 Logging

The firewall MUST be configured in such a way that it logs the following events at minimum:

- rejected network connections (source and destination IP addresses, source and destination ports or ICMP/ICMPv6 type, date, time)
- failed attempts to access system resources due to improper authentication, lack of authorisation or non-existent resources
- error messages of the firewall services
- general system error messages

If security proxies are used, security violations and violations of access control lists (ACLs) MUST be logged appropriately. At minimum, this should include the type of protocol violation or ACL violation, the source and destination IP addresses, the source and destination ports, the service, the date and time and the duration of the connection (if required).

When a user provides authentication for the security proxy, the authentication data or only the information on a failed authentication attempt MUST also be logged.

The persons in charge MUST ensure that all legal framework conditions are complied with during logging.

NET.3.2.A1 Protection Against Fragmentation Attacks on the Packet Filter

Protection mechanisms MUST be enabled on the packet filter in order to fend off IPv4 and IPv6 fragmentation attacks.

NET.3.2.A11 Installing Updates and Patches

The persons in charge MUST obtain information on known vulnerabilities. Updates and patches MUST be installed as quickly as possible. Before this occurs, a test system SHOULD be used to check whether the security updates are compatible and do not cause any errors. As long as no patches are available in the event of known vulnerabilities, other appropriate safeguards MUST be implemented in order to protect the firewall.

It MUST be ensured that patches and updates are only obtained from trustworthy sources. This MUST also be observed regarding related services within the firewall system.

NET.3.2.A12 Procedure in the Event of Security Incidents

The reaction required in the event of a detected attack **MUST** be defined. The tasks and authorities for the employees affected **MUST** be clearly defined. Additional information on this can be found in DER.2.1 *Security Incident Handling*.

NET.3.2.A13 Regular Backups

Backups of the firewall system **MUST** be performed at regular intervals. The system **MUST** also be backed up before a new firewall is installed or a firewall's configuration is changed. If backed-up data is imported back into the system, the security-relevant files (such as access lists, password files, and filter rules) **MUST** correspond to the configuration status required from a security point of view.

NET.3.2.A14 Operational Documentation

The operational tasks of a firewall **MUST** be documented in a transparent manner. All configuration changes and security-relevant tasks **MUST** be documented, particularly changes to the system services and the rule set of the firewall. The documentation **MUST** be protected against unauthorised access. Changes to the configuration **MUST** also be logged automatically whenever possible.

NET.3.2.A15 Procuring a Firewall

Prior to procuring a firewall, a requirements list **MUST** be drawn up that can be used to evaluate the products available on the market. It **SHOULD** be ensured that the desired security level of the organisation can be achieved with the firewall. Hence, the procurement process **MUST** be based on the requirements from the security policy.

If IPv6 is used, the packet filter **MUST** check the IPv6 extension headers. Furthermore, it **MUST** be possible to configure IPv6 adequately for IPv4.

Standard Requirements

For module NET.3.2 *Firewall*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

NET.3.2.A16 Creation of a P-A-P Structure

A packet filter – application level gateway – packet filter (P-A-P) structure **SHOULD** consist of several components, each with the appropriate hardware and software. Security proxies **SHOULD** exist for the most important protocols used and generic security proxies (at minimum) **MUST** be present for TCP and UDP. The security proxies **SHOULD** also be executed in a secured runtime environment of the operating system.

NET.3.2.A17 Disabling IPv4 or IPv6

If the IPv4 or IPv6 protocol is not required in a network segment, it **SHOULD** be disabled at the respective firewall network access point (e.g. at the corresponding firewall interface). If the IPv4 or IPv6 protocol is not required or used at all, it **SHOULD** be disabled completely on the firewall.

NET.3.2.A18 Administration Using a Separate Management Network

Firewalls SHOULD ONLY be administered using a separate management network (out-of-band management). If one exists, the administration interface via the actual data network (in-band) MUST be disabled. The communication in the management network SHOULD be restricted to a few management protocols with precisely defined sources and destinations using management firewalls (see NET.1.1 *Network Architecture and Design*). The available security mechanisms of the management protocols used for authentication, integrity protection and encryption SHOULD be enabled and all insecure management protocols SHOULD be disabled (see NET.1.2 *Network Management*).

NET.3.2.A19 Protection Against TCP SYN Flooding, UDP Packet Storms and Sequence Number Guessing on the Packet Filter

On the packet filter protecting server services that are available from non-trusted networks, a limit SHOULD be configured for semi-open and open connections.

On the packet filter protecting server services that are available from less or non-trustworthy networks, rate limits SHOULD be set for UDP data streams.

On the outer packet filter, random generation of initial sequence numbers (ISN) SHOULD be enabled for outgoing connections for TCP unless this is already implemented by security proxies.

NET.3.2.A20 Protection of Fundamental Internet Protocols

In order to communicate with the Internet, the protocols HTTP, SMTP and DNS (including their encrypted versions) SHOULD be routed via protocol-specific security proxies.

NET.3.2.A21 Temporary Decryption of Data Traffic

Encrypted connections in non-trusted networks SHOULD be decrypted temporarily in order to verify the protocol and check the data for malware. In so doing, the legal framework conditions MUST be taken into consideration.

The component that temporarily decrypts the data traffic SHOULD prevent the use of legacy encryption options (e.g. SSL) and cryptographic algorithms (e.g. DES, MD5, SHA1).

The TLS proxy SHOULD also be able to check whether certificates are trustworthy. If a certificate is not trustworthy, it SHOULD be possible to reject the connection. It SHOULD be possible to subsequently integrate proprietary certificates in order to be able to configure and check “internal” root certificates, as well. Pre-configured certificates SHOULD be checked and removed if they are not required.

NET.3.2.A22 Secure Time Synchronisation

Secure time synchronisation SHOULD be performed with a Network Time Protocol (NTP) server. The firewall SHOULD not permit external time synchronisation. Additional requirements can be found in module NET.1.2 *Network Management*.

NET.3.2.A23 System Monitoring and Evaluation

Firewalls SHOULD be integrated into an appropriate system monitoring concept. Furthermore, a process SHOULD be defined to control how logged data is to be evaluated and which protocols are to be evaluated regularly, sporadically or only when there is a reason to do so. It SHOULD consistently be monitored whether the firewall itself and the services operated on it are working properly. Should errors occur or thresholds be exceeded, the operating personnel

SHOULD be alarmed. Furthermore, alarm messages SHOULD be generated automatically for defined events. Logged data or status messages SHOULD only be transmitted using secure communication channels.

NET.3.2.A24 Audits and Penetration Tests

The firewall structure SHOULD be checked for known security issues at regular intervals. Regular penetration tests and audits SHOULD be performed.

Requirements in Case of Increased Protection Needs

Generic suggestions for module XXX are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

NET.3.2.A25 Advanced Integrity Protection for Configuration Files (CI)

In the event of a system crash, it SHOULD be ensured that no legacy or incorrect configurations (among other things, access lists) are used. This SHOULD also apply if an attacker manages to restart the firewall.

NET.3.2.A26 Outsourcing of Functional Extensions to Dedicated Hardware (CIA)

In order to further minimise the risk of attacks, an organisation SHOULD outsource functional extensions of the firewall to dedicated hardware and software.

NET.3.2.A27 Use of Different Firewall Operating Systems and Products in Multi-Layer Firewall Architecture (CI)

In multi-layer firewall architecture, different operating systems and products SHOULD be used for the outer and inner firewalls so that the potential vulnerability of an operating system or product has less far-reaching effects.

NET.3.2.A28 Central Filtering of Active Content (CI)

Active content SHOULD be filtered in a centralised manner according to the security objectives of the organisation. To this end, the encrypted data traffic SHOULD also be decrypted. The required security proxies SHOULD support the filtering of active content.

NET.3.2.A29 Use of High-Availability Solutions (A)

The packet filter and application level gateway SHOULD be designed to ensure high availability. Furthermore, there SHOULD be two independent access options to the external network (e.g. Internet access through two different providers). Internal and external routers and any other active components involved (e.g. switches) that may cause a loss of availability SHOULD also be designed to ensure high availability.

Even after an automatic failover, the firewall structure SHOULD comply with the security requirements of the security policy (fail safe and fail secure).

Function monitoring SHOULD be based on numerous parameters, not a single criterion. Log files and warnings of the high-availability solution SHOULD be checked at regular intervals.

NET.3.2.A30 Bandwidth Management for Critical Applications and Services (A)

In order to ensure bandwidth management for critical applications and services, packet filters with a corresponding bandwidth management function SHOULD be used at network gateways and at the gateways between different security zones.

NET.3.2.A31 Use of Certified Products (CI)

Firewalls with a Common Criteria security evaluation of at least EAL4 SHOULD be used.

Additional Information

For more information about threats and security safeguards for module NET.3.2 *Firewall*, see the following publications, among others:

[BSICS112]	Next Generation Firewalls: Empfehlung von Einsatzmöglichkeiten für den normalen Schutzbedarf [Recommendation of Possible Applications for Normal Protection Requirements], BSI publications on cyber security (BSI-CS 112), Version 1.0, April 2015, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/infos/20150407_BSI_Empfehlung_NGFW.html , last accessed on 05.10.2018
[ISILANA]	Secure Connection of Local Networks to the Internet (ISi-LANA): Federal Office for Information Security (BSI), Version 2.1, August 2014 https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-LANA/lana_node.html , last accessed on 05.10.2018
[NIST80041]	Guidelines on Firewalls and Firewall Policy: NIST Special Publication 800-41, Revision 1, September 2009, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf , last accessed on 05.10.2018
[TR21022]	Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths: Part 2: Use of Transport Layer Security (TLS), Federal Office for Information Security (BSI), January 2017, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html , last accessed on 24.08.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.3.2 *Firewall*:

G 0.8 Failure or Disruption of the Power Supply

G 0.9 Failure or Disruption of Communication Networks

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.24 Destruction of Devices or Storage Media
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.27 Lack of Resources
- G 0.28 Software Vulnerabilities or Errors
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation
- G 0.39 Malware
- G 0.40 Denial of Service
- G 0.41 Sabotage
- G 0.43 Attack with Specially Crafted Messages
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats	G 0. 8	G 0. 9	G 0. 14	G 0. 18	G 0. 19	G 0. 20	G 0. 21	G 0. 22	G 0. 23	G 0. 24	G 0. 25	G 0. 26	G 0. 27	G 0. 28	G 0. 29	G 0. 30	G 0. 31	G 0. 32	G 0. 39	G 0. 40	G 0. 41	G 0. 43	G 0. 45	G 0. 46
NET.3.2. A1			X									X												
NET.3.2. A2		X		X				X											X	X	X	X		X
NET.3.2. A3		X		X				X											X	X	X	X		X
NET.3.2. A4	X	X		X		X	X	X		X	X		X		X		X				X		X	X
NET.3.2. A5							X				X										X			X
NET.3.2. A6	X			X		X	X	X		X			X		X		X				X		X	X
NET.3.2. A7	X									X														
NET.3.2. A8							X			X											X	X		
NET.3.2. A9						X	X								X	X	X	X			X	X	X	X
NET.3.2. A10				X																	X	X		
NET.3.2. A11					X	X			X				X								X			
NET.3.2. A12			X																		X			
NET.3.2. A13																							X	

NET.3.2. A14			X	X																
NET.3.2. A15			X	X																
NET.3.2. A16		X	X		X	X								X	X					
NET.3.2. A17							X													
NET.3.2. A18	X						X				X									
NET.3.2. A19														X	X					
NET.3.2. A20		X	X							X							X			
NET.3.2. A21						X										X	X			
NET.3.2. A22					X	X					X	X	X	X		X	X	X	X	
NET.3.2. A23	X	X					X		X	X	X				X	X				
NET.3.2. A24					X	X	X			X						X				
NET.3.2. A25			X		X	X	X			X								X	X	
NET.3.2. A26			X						X	X										
NET.3.2. A27		X	X		X	X			X	X										
NET.3.2. A28																X			X	
NET.3.2. A29	X	X							X											



NET.3.3: VPN

Description

Introduction

With the help of virtual private networks (VPNs), it is possible to implement security safeguards to transmit sensitive data using untrustworthy networks like the Internet. A VPN is a network that is physically operated within another network (e.g. the Internet), but logically separated from this network. VPNs can protect the integrity and confidentiality of data with the help of cryptographic procedures. This also makes secure authentication possible for the communication partners even if several networks or computers are connected using leased lines or public networks.

Objective

This module defines requirements for the targeted and secure planning, implementation and operation of a VPN.

Not in Scope

For the purposes of this module, a VPN is a network that is physically operated within another network, but logically separated from this network. The *VPN* module does not deal with basics of secure networks (see NET.1.1 *Network Architecture and Design*). Moreover, it does not cover all processes connected to the operation of a VPN. In addition, the modules OPS.1.1.3 *Patch and Change Management*, ORP.3 *Awareness and Training*, CON.1 *Crypto Concept*, CON.3 *Backup Concept*, DER.4 *Business Continuity Management* and OPS.2.4 *Remote Maintenance* must be considered above all.

The present module must be used for any type of remote access to the information domain. This includes connections established using data networks (e.g. site-to-site, end-to-end, or remote-access VPNs) and telecommunications connections (e.g. analogue switched lines, ISDN, or mobile phones). This module only covers VPN systems for layers 2 (data link layer) to 4 (transport layer) of the Open Systems Interconnection (OSI) model.

Recommendations on how to configure the operating systems of the VPN end points are not part of this module either. Corresponding requirements are included in the modules SYS.1.1 *General Server* and SYS.2.1 *General Client*, as well as in the relevant operating-system-specific modules of the *IT-Grundschutz Compendium*.

Threat Landscape

For module NET.3.3 *VPN*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Inadequate Planning and Regulation of VPN Usage

If a VPN is not carefully planned, designed or configured, vulnerabilities that impair all IT systems connected to the VPN may occur. Attackers will thus be able to access confidential information of the organisation.

For example, inadequate planning and regulation of VPNs may result in users who have not been trained properly and thus use the VPN in an insecure environment or use an insecure client to connect. This in turn may enable attackers to access the entire company network.

Attacks may also be detected too late if regular checks of VPN access were inadequately planned. It will thus not be possible to respond in time, and an attacker may steal data or sabotage entire processes without being detected.

Insecure VPN Service Providers

VPN connections may extend into critical areas of the network. If the organisation uses a VPN service provider that was not selected carefully, this could result in the entire network of the organisation becoming insecure. For example, VPN access provided by the service provider in an insecure manner could be used by attackers to steal specific information.

Problems with Local Storage of VPN Authentication Data

Many VPN clients for remote access allow local storage of the data required for authentication so that the users do not need to enter such data again when re-establishing the connection. If an attacker is able to access the VPN client, they might obtain this data and log into the network as a legitimate user. Then, the attacker may access the local networks and the organisational information and services located there.

Insecure Configuration of VPN clients for Remote Access

If a VPN client is configured insecurely, the users may use its security mechanisms incorrectly (or not at all). They could also change the configuration of the client. Due to insecure configuration, software installed by the user may also threaten the security of the VPN client.

Insecure Default Settings on VPN Components

The default settings of VPN components do not always exhibit the characteristics of a secure installation. In many cases, the manufacturers pay more attention to user-friendliness and problem-free integration into existing systems than they do to security. If VPN components are insufficiently adapted to the actual security requirements of the organisation, this will create vulnerabilities and corresponding points of attack. For example, the entire VPN (and thus also the internal network of the organisation) will be open to attack if the default passwords of the manufacturer are not changed.

Theft of Mobile End Devices with VPN Clients

Mobile end devices are often stolen or lost. This poses the risk that attackers may use the VPN connection established with such devices to access the internal network of the organisation. In many cases, there are no loss reporting processes in place and a stolen laptop (for example) is not reported to the responsible entity within the organisation in due time. The attacker may therefore access the internal network and copy a good deal of sensitive information without being detected for a long time.

Requirements

The specific requirements of module NET.3.3 VPN are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	Chief Information Security Officer (CISO)

Basic Requirements

For module NET.3.3 VPN, the following requirements **MUST** be implemented as a matter of priority:

NET.3.3.A1 Planning the Use of VPNs

Careful planning **MUST** be carried out before implementing a VPN. Here, the responsibilities for operating the VPN **MUST** be defined. User groups and their authorisations **MUST** also be planned for the VPN. Moreover, it **MUST** be defined how granted, changed or withdrawn access authorisations are to be documented.

NET.3.3.A2 Selecting a VPN Service Provider [Chief Information Security Officer (CISO)] (I)

Service level agreements (SLAs) **MUST** be negotiated and documented in writing with a VPN service provider. It **MUST** be checked regularly that the VPN service provider is complying with the agreed SLAs.

NET.3.3.A3 Secure Installation of VPN End Devices

The underlying operating system of the VPN platform **MUST** be securely configured. If an appliance is used, there **MUST** be a valid maintenance contract for this. It **MUST** be ensured that VPN components are only installed by qualified personnel. The installation of the VPN components and any deviations from the planning specifications **SHOULD** be documented. The functions and the selected security mechanisms of the VPN **MUST** be checked before commissioning.

NET.3.3.A4 Secure Configuration of a VPN

A secure configuration **MUST** be specified for VPN clients, VPN servers and VPN connections. This **SHOULD** be documented appropriately. The administrator in charge **MUST** check regularly that the configuration is still safe and adapt it to all IT systems (if applicable).

NET.3.3.A5 Blocking Unneeded VPN Accounts

It **MUST** be checked regularly that only authorised IT systems and users can access the VPN. VPN access that is no longer required **MUST** be deactivated promptly. VPN access **MUST** be limited to the usage time required.

Standard Requirements

For module NET.3.3 *VPN*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

NET.3.3.A6 Analysis of VPN Requirements

A requirements analysis SHOULD be performed to determine the scenarios of use for the relevant VPN and use them as a basis for deriving the requirements for the required hardware of software components. The requirements analysis SHOULD take into consideration the following:

- business processes
- access routes
- identification and authentication procedures
- users and user authorisations
- responsibilities
- reporting channels

NET.3.3.A7 Planning the Technical VPN Implementation

In addition to the general planning (see NET.3.3.A1 *Planning the Use of VPNs*), the technical aspects of a VPN SHOULD also be planned carefully. The encryption methods, VPN end points, permitted access protocols, services and resources SHOULD be specified for the VPN. Furthermore, the sub-networks (see NET.1.1 *Network Architecture and Design*) that can be accessed via VPN SHOULD be defined.

NET.3.3.A8 Drawing Up a Security Policy for VPN Usage

A security policy for the use of VPNs SHOULD be drawn up and communicated to the employees. The security safeguards SHOULD be explained within the scope of training courses. If VPN access is set up for an employee, they SHOULD be issued an information sheet detailing the most important VPN security mechanisms. All VPN users SHOULD be obligated to comply with the security policy.

NET.3.3.A9 Selection of Suitable VPN Products

When selecting VPN products, the requirements of the organisations regarding the networking of different locations and the connection of mobile employees and teleworkers SHOULD be considered.

NET.3.3.A10 Secure Operation of a VPN

An operational concept SHOULD be created for VPNs. This SHOULD include the aspects of quality management, monitoring, maintenance, training and authorisation.

NET.3.3.A11 Secure Integration of an External Network

If a VPN is used to integrate an external network, secure state-of-the-art authentication and encryption procedures with sufficient key lengths SHOULD be used. In addition, the selected

procedure for exchanging keys SHOULD correspond to the state of the art. It SHOULD be ensured that VPN connections are only created between the relevant IT systems and services. The tunnel protocols used for this SHOULD be suitable for such use.

NET.3.3.A12 User and Access Management for Remote Access VPNs

In cases involving remote access VPNs, central and consistent user and access management SHOULD be ensured. The authentication procedures used SHOULD meet the requirements of module ORP.4 *Identity and Access Management*.

If independent servers are used for user and access management, it SHOULD be ensured that they are configured and operated in a secure manner and in compliance with the requirements of module ORP.4 *Identity and Access Management*. Moreover, the servers used SHOULD be protected against unauthorised access.

NET.3.3.A13 Integration of VPN Components into a Firewall

The VPN components SHOULD be integrated into the firewall so that the data traffic can be controlled and filtered effectively. It SHOULD be documented how the VPN components are integrated into the firewall.

Requirements in Case of Increased Protection Needs

For module NET.3.3 *VPN* there are no Requirements in Case of Increased Protection Needs.

Additional Information

For more information about threats and security safeguards for module NET.3.3 *VPN*, see the following publications, among others:

[27033-5]	ISO/IEC 27033-5:2013: Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs), International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, August 2013
[ISIVPN]	Virtual Private Network (ISi-VPN): BSI Policy for Internet Security (ISi-L), Federal Office for Information Security (BSI), 2009, https://www.bsi.bund.de/DE/Themen/StandardsKriterien/ISi-Reihe/ISi-VPN/vpn_node.html , last accessed on 05.10.2018
[NIST80077]	Guide to IPsec VPNs: NIST Special Publication 800-77, December 2005, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-77.pdf , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.3.3 *VPN*:

G 0.9 Failure or Disruption of Communication Networks

G 0.11 Failure or Disruption of Service Providers

G 0.14 Interception of Information / Espionage

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.28 Software Vulnerabilities or Errors

G 0.32 Misuse of Authorisation

G 0.40 Denial of Service

G 0.43 Attack with Specially Crafted Messages

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.9	G 0.11	G 0.14	G 0.18	G 0.19	G 0.22	G 0.23	G 0.28	G 0.32	G 0.40	G 0.43	G 0.46
NET.3.3.A1				X					X			
NET.3.3.A2		X										
NET.3.3.A3	X			X								
NET.3.3.A4			X		X	X	X		X			
NET.3.3.A5								X				
NET.3.3.A6				X			X		X			
NET.3.3.A7			X		X	X	X				X	X
NET.3.3.A8				X								
NET.3.3.A9	X	X								X		
NET.3.3.A10			X		X	X					X	X
NET.3.3.A11	X	X								X		
NET.3.3.A12									X			
NET.3.3.A13			X		X	X					X	X



NET.4.1: Telecommunications Systems

Description

Introduction

By using a telecommunication system, also known as a PBX system, an organisation's telephones can be connected internally and to an external public telephone network. Due to the increasing integration of IT and telecommunications, PBXs can be both analogue and IP-based. Hybrid systems represent a combination of a classic TDM-based telecommunications solution with a VoIP system. With a hybrid system, classic digital or analogue telephony and VoIP can be used simultaneously.

Along with voice telephony, additional services may be used depending on the end devices connected. For example, PBX systems can be used to transmit data, texts, graphics, and moving images. The information can be transmitted analogously or digitally using wired or wireless transmission media. Depending on the connection and the data networks used, different versions of PBX systems may be used in an organisation.

Objective

This module examines the threats and requirements that apply specifically to PBX and hybrid systems. The module should be used for every PBX system.

Not in Scope

This module deals with the hazards and requirements pertaining to a PBX system. Topics that go beyond the PBX – such as hazards and requirements for individual VoIP implementations, as well as externally provided services – are covered in the corresponding modules.

The security aspects of VoIP components and voice transmission via VoIP are described in more detail in module NET.4.2 *VoIP*. Internet telephony via clients or mobile IT devices is considered in module NET 4.5 Unified Communication. If video and other data is to be transmitted instead of or in addition to voice data, the requirements of module NET 4.4 Telepresence and Video Conferencing should be taken into account.

Threat Landscape

For module NET.4.1 *Telecommunications Systems*, the following specific threats and vulnerabilities are of particular importance:

Eavesdropping on Telecommunications Systems

If telephone calls or data are transmitted in an unencrypted form, there is generally the risk of attackers eavesdropping on or reading the information. For example, attackers could tap directly into the telephone cables or eavesdrop on a PBX system connecting the callers.

In many PBX systems, callers can leave a message for the recipient if the recipient is not available by telephone at the time of the call. Some answering machines, especially those in VoIP systems, send this information in the form of an audio file attached to an e-mail. The contents of this e-mail could be directly intercepted and an attack could eavesdrop.

In addition, it is possible for third parties to listen in on calls by activating disabled features, some of which are not allowed in Germany. Silent monitoring is one example of this. Activation of such features requires more detailed knowledge of the system, which is not a serious obstacle due to the large amount of information freely available on the Internet.

Eavesdropping on Rooms Using Telecommunications Systems

As a matter of principle, it is possible to eavesdrop on rooms using microphones in end devices. Here, a distinction is made between two variants.

In the first case, the threat arises through the use of one end device. Examples could include intelligent end devices with built-in microphones – multimedia PCs, PDAs and mobile telephones, for example, but also answering machines. If corresponding functions are implemented, these end devices can be prompted to activate their built-in microphones from the public network or via the LAN. A well-known example of this is the “baby monitor” function available in some phones or answering machines.

In the second case, the functionality of a PBX system is exploited in combination with correspondingly equipped end devices. This threat arises through misuse of the "voice calling" feature in combination with the "hands-free" option. This combination can cause the system to operate like an intercom system under certain circumstances, which makes it possible to eavesdrop on a room.

Call Charge Fraud

Call charge fraud in connection with data or telecommunication servers involves transferring the cost of telephone calls or data transmissions to a third party – for example, by misusing a PBX system. A PBX system can be manipulated in various ways. On the one hand, attackers might attempt to abuse the features available on a PBX system to charge calls. Call forwarding or dial-in options that can be programmed remotely are examples of possible means of doing so. On the other hand, rights can be granted in such a way that incoming outside lines occupy outgoing outside lines. In this way, the caller can be automatically reconnected to the exchange from outside when dialling a specific number – but at the expense of the PBX operator.

Along with these technical possibilities, users can also cause fraud on their own. Using various methods, such as making telephone calls from other people's telephones, reading other people's authorisation codes (passwords), or modifying personal authorisations, attempts can be made to make calls at the expense of the employer or other employees.

Abuse of Freely Accessible Telephone Extensions

Telephones are often used without being assigned to a specific user. Some of these telephones, such as those in printer rooms, can only be accessed by a limited group of people. However, telephones are also often found in parking garages, at the entrances to access control systems, or in areas accessible to visitors. If these telephones have an electronic telephone book containing internal telephone numbers, these internal telephone numbers could be exposed to outsiders.

Requirements

The specific requirements of module NET.4.1 *Telecommunications Systems* are listed below. As a matter of principle, the Business Telephone System Manager is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Business Telephone System Manager
Further Roles	Head of Personnel, IT Operation Department, Head of IT

Basic Requirements

For module NET.4.1 *Telecommunications Systems*, the following requirements **MUST** be implemented as a matter of priority:

NET.4.1.A1 Requirements Analysis and Planning for PBX Systems [IT Operation Department, Head of IT]

Prior to the procurement or expansion of a PBX system, a requirements analysis **MUST** be carried out. This analysis **MUST** determine the functions the PBX system should offer. In addition to the type of PBX, the number of connections, potential extensibility, basic security functions and requirements pertaining to the key security objectives **MUST** also be taken into account. In addition, support and maintenance contracts for the PBX **MUST** be taken into account as required. Based on the requirements determined, the use of the PBX **MUST** then be planned and documented. The requirements and planning **MUST** be coordinated with the corresponding persons responsible for IT.

NET.4.1.A2 Selection of PBX Service Providers [Head of IT]

In order to be able to make calls to persons who are not connected to the organisation's own PBX, a PBX service provider **MUST** be contracted. The requirements for the PBX, the security policy and contractual and financial aspects **MUST** be taken into account. All services agreed **MUST** be specified clearly and concisely in writing.

NET.4.1.A3 Change of Preset Passwords

Standard passwords **MUST** be replaced by sufficiently strong passwords. Predefined logins **MUST** be changed. The changes **MUST** be made before the PBX is put into operation.

NET.4.1.A4 Protecting Remote Access

Whether internal or external remote access points are required for the PBX system **MUST** be checked. External remote maintenance **SHOULD** be prevented if possible. Any unnecessary remote access points **MUST** be disabled. All other remote access **MUST** be protected from unauthorised access and restricted to the necessary persons.

NET.4.1.A5 Logging for PBX Systems

Suitable data **MUST** be recorded for PBX systems and evaluated internally if necessary. Additionally, all evaluation procedures, data transmissions, data access and system-related interventions that involve program modifications **MUST** be logged. All administration work on the PBX system **MUST** be logged. The logged information **MUST** be checked regularly.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module NET.4.1 *Telecommunications Systems*: They **SHOULD** be implemented as a matter of principle.

NET.4.1.A6 Creating a Security Policy for PBX Systems [Head of IT]

A security policy **SHOULD** be created for the PBX system based on the organisation-wide security policy. The security policy **SHOULD** include basic statements about confidentiality, availability and integrity. All persons and groups involved in the procurement, design, implementation, and operation of the PBX system **SHOULD** be familiar with the security policy for PBX systems and use it as the basis for their work. The central security requirements for the PBX system and the security level to be achieved **SHOULD** be included in the organisation-wide information security policy.

NET.4.1.A7 Installation of the PBX System

The PBX system **SHOULD** be located in a suitable room. The interfaces on the PBX, especially those that are unused, **SHOULD** be suitably protected.

NET.4.1.A8 Limitation and Blocking of Unnecessary or Security-Critical Features

The scope of available features **SHOULD** be limited to the necessary minimum. Only the features needed **SHOULD** be activated. The features not required or deemed critical due to their potential for being misused **SHOULD** be disabled on the central system as far as possible. Additional protective safeguards **SHOULD** be implemented for the confidential data stored on or retrievable from the end devices.

NET.4.1.A9 Training on the Secure Use of PBX Systems [Head of Personnel, Head of IT]

The users of the PBX system **SHOULD** be instructed in the correct use of services and devices. The users of the PBX system **SHOULD** be provided with all required documents regarding the operation of the corresponding end devices. Any abnormal behaviour of the PBX system **SHOULD** be reported to the relevant person in charge.

NET.4.1.A10 Documentation and Revision of the PBX System Configuration [Head of IT]

The PBX system configuration **SHOULD** be suitably documented and updated. The PBX system configuration **MUST** be evaluated at regular intervals. The results of the evaluation **SHOULD** at least be presented to the Chief Information Security Officer, the person responsible for IT, or another specifically appointed person.

NET.4.1.A11 Decommissioning PBX Systems and Devices [Head of IT]

The disposal of PBXs and connected PBX devices SHOULD be considered in the general security policy. Data stored on PBX systems or devices SHOULD be securely erased before disposal.

NET.4.1.A12 Backup of Configuration Files

The configuration and application data of the PBX system used SHOULD be backed up during the initial setup and then on a regular basis, particularly after modifications. Whether the backups of PBX systems can actually be used as a basis for system recovery SHOULD be regularly checked and documented.

A backup concept SHOULD be drawn up for PBX systems and coordinated with the general data protection concepts for servers and network components.

NET.4.1.A13 Acquisition of PBX Units

The results of the requirements analysis and the planning SHOULD be included in the procurement of the PBX systems. When procuring a classic PBX system, the need for both digital and analogue subscriber connections SHOULD be considered. Furthermore, existing communication systems and components SHOULD be taken into account in the procurement process.

NET.4.1.A14 Contingency Planning for PBX Systems

A contingency plan SHOULD be drawn up for the PBX system. This SHOULD be integrated in the organisation's contingency concept. Regular emergency drills SHOULD be carried out with regard to the PBX systems.

NET.4.1.A15 Emergency Calls in the Event of a PBX System Failure

It SHOULD be ensured that emergency calls can be made from the organisation even in the event of a PBX system failure. The emergency call facilities SHOULD be accessible and sufficiently close to all rooms.

NET.4.1.A16 Securing Telephony End Devices in Openly Accessible Rooms

The range of functions SHOULD be restricted for telephony end devices set up in openly accessible rooms. If this is not possible, the end device SHOULD be protected against unauthorised access in a suitable manner.

Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.4.1 *Telecommunications Systems* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

NET.4.1.A17 Maintenance of PBX Systems (CI)

The devices for maintaining and configuring the PBX SHOULD be secured with passwords or PINs. The data connection SHOULD be encrypted for IP-based access to the PBX system.

NET.4.1.A18 Increased Access Protection (CI)

The PBX system SHOULD be located in a separate and suitably secured room. Site and data access to PBX systems SHOULD be restricted to a specific group of people. External staff SHOULD ONLY have supervised access to the system.

NET.4.1.A19 Redundant Connections (A)

The PBX system connection SHOULD be redundant. An additional PSTN connection SHOULD be available for IP-based PBX systems.

Additional Information

For more information about threats and security safeguards for module NET.4.1 *Telecommunications Systems*, see the following publications, among others:

[TL2103]	Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf: BSI-TL-02103 - Version 2.0, Federal Office for Information Security (BSI), 2014, https://www.bsi.bund.de/DE/Publikationen/TL-sichere-TK-Anlagen/TL02103_hm.html , last accessed on 05.10.2018
----------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.4.1 *Telecommunications Systems*:

- G 0.9 Failure or Disruption of Communication Networks
- G 0.11 Failure or Disruption of Service Providers
- G 0.14 Interception of Information / Espionage
- G 0.15 Eavesdropping
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.21 Manipulation with Hardware or Software
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.42 Social Engineering

Elementary Threats Requirements	G 0.9	G 0.11	G 0.14	G 0.15	G 0.18	G 0.19	G 0.21	G 0.25	G 0.26	G 0.30	G 0.31	G 0.42
NET.4.1.A1		X			X							
NET.4.1.A2	X	X			X							
NET.4.1.A3			X	X		X	X			X		
NET.4.1.A4			X	X		X	X			X		
NET.4.1.A5				X							X	
NET.4.1.A6					X	X					X	
NET.4.1.A7			X	X		X	X	X		X		
NET.4.1.A8			X	X		X					X	X
NET.4.1.A9											X	X
NET.4.1.A10			X						X			
NET.4.1.A11						X						
NET.4.1.A12						X						
NET.4.1.A13	X				X							
NET.4.1.A14	X								X			
NET.4.1.A15	X	X										
NET.4.1.A16							X			X		
NET.4.1.A17				X		X	X			X		
NET.4.1.A18							X			X		
NET.4.1.A19	X	X						X				



NET.4.2: VoIP

Description

Introduction

Voice over IP (VoIP) refers to telephony over data networks, in particular over the Internet. Special signalling protocols are used to transmit signalling information, such as when making a call. The actual payload, such as voice or video data, is transmitted with the aid of a media transport protocol. Both protocols are required to establish and maintain a multimedia connection. Some procedures use only one protocol for signalling and transporting the media.

Objective

This module examines the security aspects of the end devices and switching units (middleware). The functionality of the components described here is the same as for the telecommunication components described in module NET 4.1 *Telecommunication Systems*.

Not in Scope

This module examines the security aspects of VoIP components and voice transmission via VoIP. It also applies to situations in which circuit-switching telecommunications systems exchange information using a data network.

The specific threats and requirements of classic PBX systems and hybrid systems are considered in module NET 4.1 *Telecommunications Systems*. Internet telephony via clients or mobile IT devices is considered in module NET 4.5 *Unified Communication*. If video and other data is to be transmitted instead of or in addition to voice data, the requirements of module NET 4.4 *Telepresence and Video Conferencing* should be taken into account.

VoIP software is often operated on standard IT systems rather than dedicated hardware. If soft-phones are installed on clients, the requirements of module SYS.2.1 *General Client* and the operating-system-specific modules should be taken into account. If software for VoIP is operated on servers, the requirements of module SYS.1.1 *General Server* should be met in addition to the requirements of the operating-system-specific modules.

Threat Landscape

For module 4.2 *VoIP*, the following specific threats and vulnerabilities are of particular importance:

Incorrect Configuration of VoIP Middleware

A VoIP-based telephone system can be affected by faulty configurations in the same manner as a circuit-switching telephone solution. Telephone users could be assigned incorrect telephone numbers, or the entire telephone infrastructure could fail. Even rather minor errors, such as a name spelled incorrectly in the telephone book, cannot be ruled out.

Several IT systems are usually involved when communicating via VoIP. If SIP is used as the initialisation protocol, systems such as registrars, SIP proxy servers, and location servers are typically needed for communication. If the VoIP infrastructure changes, all the related IT systems must be adapted, which can easily lead to configuration errors. Even when all services are located on one server, they often need to be configured individually. An incorrect change made to just one system could possibly result in the inability to use the entire telephone infrastructure.

Incorrect Configuration of VoIP Components

Regardless of whether the VoIP components come in the form of dedicated hardware (appliances) or software-based systems, configuration is crucial for the correct functioning of the system. In addition to the signalling settings specified during the planning phase, the transmission method plays an important role for the media streams. Applying a compression method can reduce the size of the data packets that contain voice information.

If an unsuitable method is used and voice information is compressed too much, the voice quality often deteriorates. If, however, a method that does not compress the data enough is selected, the stream of information will not be adequately reduced and the data network can become overloaded.

Eavesdropping on Telephone Calls

If telephone calls or data are transmitted in an unencrypted form, there is a general risk of attackers eavesdropping on or reading the information. For example, attackers could tap directly into the telephone cables or eavesdrop on a PBX system connecting the callers. With VoIP, it is even easier to eavesdrop on telephone calls and data transmissions than with classic PBXs. All voice information is transmitted in a media stream – using the Real-time Transport Protocol (RTP), for example. With techniques such as spoofing and sniffing, attackers can use all types of attacks on data networks for VoIP.

In many PBX systems, callers can leave a message for recipients who are not available at the time of the call. Some answering machines, especially those in VoIP systems, send this information in the form of an audio file attached to an e-mail. The contents of this e-mail could be directly intercepted and an attack could eavesdrop.

Abuse of Freely Accessible Telephone Extensions

Telephones are often used without being assigned to a specific user. Some of these telephones, such as those found in printer rooms, can only be accessed by a limited group of people. However, telephones are also often found in parking garages, at the entrances to access control systems, or in areas accessible to visitors. If these telephones have an electronic telephone book containing internal telephone numbers, these internal telephone numbers could be exposed to outsiders.

When VoIP telephones are used in freely accessible areas, additional aspects must be taken into consideration. VoIP telephones consist primarily of software and are often operated in data

networks that are also used for other IT applications. An attacker could therefore attempt to exploit vulnerabilities in the VoIP software or install malware when he/she has direct access to the device.

VoIP telephones need to be connected to a data network. An attacker could connect a mobile IT system to this network and access it under some circumstances, even though it is protected from the outside by a firewall. He/she could then exploit this access to initiate attacks on confidentiality, integrity, and availability.

Requirements

The specific requirements of module NET.4.2 *VoIP* are listed below. As a matter of principle, the IT Operation Department is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	IT Operation Department
Further Roles	User, Head of IT

Basic Requirements

For module NET.4.2 *VoIP*, the following requirements **MUST** be implemented as a matter of priority:

NET.4.2.A1 Planning the Use of VoIP [Head of IT]

The conditions required for the use of VoIP **MUST** be specified. Among other things, it **MUST** be decided whether to switch completely or partially to VoIP. Special requirements on the availability of VoIP or the confidentiality and integrity of telephone calls or signalling information **SHOULD** be determined in advance. Suitable signalling and media transport protocols **MUST** be selected prior to use.

It **SHOULD** be decided whether and how the VoIP infrastructure should be connected to public (data) networks. The capacities and design of existing data networks **SHOULD** be taken into account during planning.

NET.4.2.A2 Secure Administration of VoIP Middleware [Head of IT]

An administration concept **MUST** be created that contains a role concept with different authorisation levels. The software components used **MUST** receive regular updates from trusted sources.

NET.4.2.A3 Secure Administration and Configuration of VoIP End Devices

End device functions that are not required **MUST** be deactivated. The configuration settings **MUST NOT** be changed without authorisation. All the end device security functions **SHOULD** be tested before productive use. The software components used **MUST** receive regular updates from trusted sources. The security mechanisms and parameters used **SHOULD** be documented.

NET.4.2.A4 Restricting Accessibility via VoIP [Head of IT]

It **MUST** be decided how external callers will be able to access the VoIP architecture. IT systems from insecure networks **MUST** be prevented from establishing direct data connections to the organisation's VoIP components. If all incoming and outgoing connections are to be concentrated via a central IT system, it **SHOULD** be ensured that all signalling and voice information between the public and private data networks is only exchanged via this authorised concentrator.

NET.4.2.A5 Secure Configuration of VoIP Middleware

The VoIP components **MUST** be configured such that the protection needs are adequately satisfied. The default configurations of the VoIP middleware **MUST** be adapted before the initial productive operation. All installation and configuration steps **SHOULD** be documented in such a way that the installation and configuration can be understood and repeated by a qualified third-party expert based on the documentation. A rule governing the restricted authentication of devices and users **SHOULD** be created. All services of the VoIP middleware that are not required **MUST** be disabled.

NET.4.2.A6 Logging of VoIP Events

It **MUST** be decided which minimum information is to be logged, how long the logged data is to be kept, who will be allowed to view the logged data and under which conditions. All log data **MUST** be protected against unauthorised access.

As a matter of principle, all security-relevant system events **MUST** be logged. The log data **SHOULD** be evaluated promptly.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module NET.4.2 *VoIP*: They **SHOULD** be implemented as a matter of principle.

NET.4.2.A7 Drawing up a Security Policy for VoIP

The central security requirements for VoIP and the security level to be achieved **SHOULD** be included in the organisation-wide information security policy. This security policy **SHOULD** detail all the general security-related requirements in concrete terms. In addition, the policy **SHOULD** regulate the requirements for the operation and use of VoIP components. The VoIP security policy **SHOULD** be available and known by all persons and groups involved.

NET.4.2.A8 Encryption of VoIP

It **SHOULD** be decided whether and which voice and signalling information is to be encrypted. In general, all VoIP data packets leaving the secure LAN **SHOULD** be protected by suitable security mechanisms. Users **SHOULD** be informed about the use of VoIP encryption.

NET.4.2.A9 Selection of Suitable VoIP Components

Before VoIP components are purchased, a requirements list **SHOULD** be created. The requirements list **SHOULD** be used to evaluate the products available on the market. This requirements list **SHOULD** include all the characteristics necessary to achieve the desired security level. The manner in which the products available on the market can be evaluated according to the requirements list **SHOULD** be regulated.

NET.4.2.A10 Administrator Training on the Use of VoIP

Training measures SHOULD be designed and carried out for administrators. The measures SHOULD cover the individual application areas of VoIP administrators and typical situations in the field of error management.

NET.4.2.A11 Secure Handling of VoIP End Devices [User]

Users of VoIP end devices SHOULD be aware of the basic VoIP threats and security measures. Users SHOULD be instructed to lock the devices appropriately when they are absent. In addition, they SHOULD select suitable passwords to secure voice mails.

NET.4.2.A12 Secure Decommissioning of VoIP Components

When VoIP appliances are to be replaced or otherwise decommissioned, all security-related information SHOULD be deleted from the devices. After deleting the data, it SHOULD be checked that the data was deleted successfully. Sensitive information SHOULD also be deleted from backup media. All labels, especially on end devices, SHOULD be removed before disposal. Safeguards for deleting security-related information which are compatible with the conditions of the contract and guarantee SHOULD be clarified with manufacturers, dealers or service providers in advance.

NET.4.2.A13 Firewall Requirements When Using VoIP

It SHOULD be checked whether the existing firewall can be adapted for the use of VoIP. If this is not the case, an additional firewall SHOULD be purchased and installed.

Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.4.2 *VoIP* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

NET.4.2.A14 Encryption of Signalling (CI)

The integrity and confidentiality of signalling information SHOULD be ensured by appropriate encryption procedures. Along with the payload, authentication data SHOULD also be continuously encrypted. Access to the VoIP gateway SHOULD be restricted to the greatest possible extent with the help of VoIP addresses and H.323 identities. Additional end-to-end security mechanisms SHOULD be used for media transport and signalling. The way signalling is protected SHOULD be documented.

NET.4.2.A15 Secure Media Transport Using SRTP (CI)

Media data transmitted via the Real-Time Transport Protocol (RTP) and information transmitted to control this data via the Real-Time Streaming Protocol (RTSP) SHOULD be protected appropriately. The payload SHOULD be protected by the use of SRTP/SRTCP. The security-relevant options for implementing the protocol SHOULD be documented.

NET.4.2.A16 Network Separation for Data and VoIP (CIA)

The VoIP network SHOULD be separated from the data network. A decision SHOULD be made on how to separate the VoIP network from the data network. The manner in which devices that need to access the VoIP and data networks are to be dealt with SHOULD be regulated. VoIP

end devices in a VoIP network SHOULD ONLY be able to establish the intended VoIP connections to other IT systems.

Additional Information

For more information about threats and security safeguards for module NET.4.2 *VoIP*, see the following publications, among others:

[NITS80058]	Security Considerations for Voice Over IP Systems: NIST Special Publication 800-5
[TL2103]	Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf [Technical Guideline for Internal Organisation of Telecommunication Systems with Increased Protection Needs]: BSI-TL-02103 - Version 2.0, Federal Office for Information Security (BSI), 2014, https://www.bsi.bund.de/DE/Publikationen/TL-sichere-TK-Anlagen/TL02103_hm.html , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.4.2 *VoIP*:

G 0.9 Failure or Disruption of Communication Networks

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.19 Disclosure of Sensitive Information

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.23 Unauthorised Access to IT Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.28 Software Vulnerabilities or Errors

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.31 Incorrect Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.40 Denial of Service

G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.9	G 0.15	G 0.18	G 0.19	G 0.20	G 0.21	G 0.23	G 0.26	G 0.27	G 0.28	G 0.30	G 0.31	G 0.32	G 0.40	G 0.45	G 0.46
NET.4.2.A1	X	X	X					X	X							X
NET.4.2.A2					X	X				X	X	X			X	
NET.4.2.A3					X	X				X	X		X			
NET.4.2.A4	X						X						X	X		
NET.4.2.A5						X					X	X				
NET.4.2.A6				X		X		X	X		X					
NET.4.2.A7		X		X							X	X	X		X	X
NET.4.2.A8		X		X												X
NET.4.2.A9	X	X	X										X			
NET.4.2.A10								X				X				
NET.4.2.A11				X			X				X					
NET.4.2.A12	X								X					X		
NET.4.2.A13		X														X
NET.4.2.A14		X														X
NET.4.2.A15	X		X	X							X			X		
NET.4.2.A16	X		X	X							X			X		



NET.4.3: Fax Machines and Fax Servers

Description

Introduction

This module examines the security aspects of information transmission via standard fax machines and fax servers. The information transmitted is referred to as a fax (short for "telefax") or, more rarely, as a telecopy or facsimile. With a conventional fax machine, the content recorded on a document is scanned point by point by the transmitting machine and transmitted to a recipient. The receiver device reconstructs this content point by point and usually outputs it directly on paper.

A fax server, on the other hand, is a service that is installed on a server to enable other IT systems in a data network to send and receive faxes. Fax servers are often integrated into existing e-mail or groupware systems. It is therefore possible for incoming fax documents to be delivered to users by e-mail. Outgoing documents are relayed to the fax server either via a printer queue system or by e-mail. The document is usually sent or received as an image file between the fax server and the clients in the data network. The transmitted image file cannot be processed directly in word processing systems; this usually requires text recognition (optical character recognition) first. Documents received and processed by a fax server can usually be easily archived – for example, by the fax server service itself, by document management systems or by the groupware directly connected to the fax server service.

Objective

One aim of this module is to protect the information transmitted and processed by fax. Another objective is the protection of fax machines and fax servers against manipulation by unauthorised persons. Since the transmission medium is irrelevant for the application of this module, the requirements should also be implemented for Fax over IP.

Not in Scope

This module considers standard stand-alone fax machines and fax servers as the technical basis for sending faxes. Additional aspects of fax machines that can be found in a multifunction (or "all-in-one") device are dealt with separately in the module SYS.4.1 *Printers, Copiers, and All-in-One Devices*. To protect the information that is processed, offered, stored and transmitted on fax servers, the module SYS.1.1 *General Server* and the respective operating-system-specific modules should be considered. Information on correct archiving can be found in module OPS.1.2.2 *Archiving*.

Threat Landscape

For module NET.4.3 *Fax Machines and Fax Servers*, the following specific threats and vulnerabilities are of particular importance:

Inadequate or Incorrect Supply of Consumables

Fax machines receive fax documents and usually print them directly on paper. The smooth and uninterrupted operation of a fax machine requires the availability of consumer goods such as paper and toner in sufficient quantities. If these consumables are not available, fax documents often cannot be received. If fax documents are to be sent and insufficient consumables are available, it is not possible to print out the transmission confirmations that may be required.

Fax Transmission Errors

Many different forms of interference can occur between the sender and recipient of a fax during transmission. This can result in the fax documents to be transmitted being incomplete or illegible or not arriving at the recipient at all. Decisions based on this information may be inappropriate, which can result in significant losses or damage.

Time delays that occur because the problems have to be identified and the document has to be resent can lead to further complications. The transmitter or receiver usually has no way of influencing the transmission path in a timely manner, and thus can only wait until the interference has been rectified by a third party. In many cases, the sender even believes that the fax document has been properly transmitted to the desired addressee and the resulting problems are then detected very late.

In addition, it cannot be ruled out that a fax document may have been transmitted to the wrong recipient machine due, for example, to a faulty connection in the public telecommunications network. The wrong call number may also be dialled on the fax machine, or the direct dial keys may have been incorrectly programmed. If a fax server is used, the phone numbers may also have been entered incorrectly or stored incorrectly in the address book. As a result, confidential information may be sent to unauthorised persons.

Manipulation of Address Books and Distribution Lists

Fax machines often have address books and distribution lists. If a fax server is used, the corresponding groupware usually makes it possible to keep similar address books and distribution lists in a central location where they can be used by several users. Recipient numbers can be stored in the address books so they do not have to be re-entered each time a fax is sent. It is also possible to create a group of fax recipients via distribution lists and thus send faxes to several people at the same time.

Once programmed, recipient numbers or distribution lists are often no longer checked when a fax document is to be sent. If an unauthorised person changes the address books or distribution lists on the fax machine or in the groupware, confidential information may be sent to the wrong recipients, or the intended recipients may not receive urgent information they require. For example, a fax number could be exchanged in the address book, or another recipient could be added to the distribution list without this ever being detected.

Unauthorised Reading of Incoming Fax Transmissions

In almost all cases, it is most economical for several users to share a fax machine. Such machines are therefore usually set up in rooms that can be accessed by all employees of an organisation, such as printer rooms. As the fax machines are freely accessible, all employees can read the received faxes and thus access confidential information.

Unauthorised persons can also view confidential documents if the access rights of a fax server have not been carefully assigned. Fax servers or the connected groupware also have an address book function. If these address books are not carefully maintained and the stored addresses are not regularly checked, faxes can be sent unnoticed to other fax numbers without the ability to recall them. This is another way that confidential information can be unintentionally passed on to third parties.

Evaluation of Residual Information in Fax Machines

Depending on the technical procedure fax machines use to store, further process, or print information, varying amounts of residual information may be located in the fax machine after a fax was sent or received. The information may be obtained by an unauthorised person who gains possession of the device or the corresponding components.

Fax transmissions are stored on the hard drive of a fax server at least until they can be delivered to a recipient. Moreover, state-of-the-art operating systems use swap files that may also contain residual information. This information could be used without permission if a fax server is accessed.

Unauthorised access to fax information is also possible if a personal computer, or the fax software installed on it, are not sufficiently protected. Accessing the hard disk of a personal computer may also enable unauthorised persons to read information.

Impersonation of a False Sender on Fax Machines

Fax transmissions are a popular medium for transmitting documents that are only valid with a signature. Just as a false sender can be faked with a misleading name and letterhead, however, a fax transmission can also be manipulated. For example, signatures from other documents can be scanned and copied onto the fax document. It is not generally possible to recognise the difference between a real signature and a reproduced graphic file. A recipient who considers the information contained therein to be authentic or even legally binding can suffer related losses as a result.

Requirements

The specific requirements of module NET.4.3 *Fax Machines and Fax Servers* are listed below. As a matter of principle, the person in charge of the fax system is responsible for fulfilling these requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Person in Charge of the Fax System
---------------------	------------------------------------

Further Roles	Chief Information Security Officer (CISO), IT Operation Department, Procurement Department, User, Building Services, Supervisors
----------------------	----------------------------------------------------------------------------------------------------------------------------------

Basic Requirements

For module NET.4.3 *Fax Machines and Fax Servers*, the following requirements MUST be implemented as a matter of priority:

NET.4.3.A1 Suitable Siting of a Fax Machine [Building Services]

Fax machines MUST be installed in such a way that received faxes cannot be viewed or removed by unauthorised persons. The installation site SHOULD also be selected to ensure that an adequate number of telephone communication lines or channels are available.

NET.4.3.A2 Information on the Use of Fax Machines for All Employees [Chief Information Security Officer (CISO)]

All employees MUST be informed about the special features of transmitting information by fax and the fact that a fax message is usually only considered legally binding to a very limited extent. An instruction manual that is easy to understand MUST be available at the fax machine. Users SHOULD receive at least a quick guide on the fax client software used by the fax server. In addition, instructions on correct fax usage MUST be displayed.

NET.4.3.A3 Secure Operation of a Fax Server [IT Operation Department]

Before a fax server is put into operation, a test phase SHOULD be carried out. The configuration parameters and all the changes made to the fax server's configuration SHOULD be documented. The archiving and deletion of fax data SHOULD be regulated. In addition, the function of the connection from the fax server to the PBX system or the public telephone network MUST be checked regularly. It MUST also be ensured that the fax server only offers fax services and is not used for any other purposes. All features and communication interface access points that are not required MUST be disabled.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module NET.4.3 *Fax Machines and Fax Servers*. They SHOULD be implemented as a matter of principle.

NET.4.3.A4 Drawing Up a Security Policy for the Use of Faxes [Chief Information Security Officer (CISO)]

A security policy for fax use SHOULD be created before a corresponding device is used. The way faxes are to be forwarded to the recipients or communication partners SHOULD be defined therein. In addition, the way in which incoming and outgoing faxes are to be dealt with SHOULD be regulated. A regulation on the handling of undeliverable faxes SHOULD also be drawn up. The policy SHOULD also contain information and instructions regarding contingency planning and fallback options for fax operations.

NET.4.3.A5 Designating a Person in Charge of the Fax System [Supervisor, IT Operation Department]

A person in charge of the fax system SHOULD be designated. This person SHOULD ensure that

- the incoming faxes are distributed to the recipients
- the fax machine is supplied with the necessary consumables
- the fax consumables are disposed of in a suitable manner
- residual information is deleted
- maintenance and repair work is supervised
- the programmable destination addresses and logs are checked regularly

For this purpose, the person in charge of the fax system SHOULD be instructed appropriately. Users SHOULD be able to reach the person in charge of the fax system during working hours.

NET.4.3.A6 Procurement of Suitable Fax Machines and Servers [Procurement Department, Chief Information Security Officer (CISO)]

Before fax machines and fax servers are purchased, a requirements list SHOULD be created. The systems or components under consideration SHOULD be assessed based on this list of requirements. The requirements list for fax machines SHOULD also include security-relevant aspects such as the exchange of subscriber IDs, the output of transmission reports, error logging and journal management. In addition, appropriate additional security functions SHOULD be considered based on the protection needs at hand.

When selecting a fax server, the requirements to be met by the IT system – including the operating system, communications components and application software – SHOULD be specified and taken into consideration. The option of integrating a fax server into an existing data network and a groupware system SHOULD be considered if necessary.

NET.4.3.A7 Suitable Labelling of Outgoing Fax Transmissions [User]

The sender and the desired recipient SHOULD be visible on all outgoing faxes. If this information cannot be obtained from the document sent, a standardised fax cover sheet SHOULD be used. All the information to be entered on the fax cover sheet SHOULD be selected in an appropriate way. In general, the fax cover sheet SHOULD include at least the name of the organisation of the sender, the contact person, the date, the number of pages and an indication of how urgent the fax is. In addition, the fax cover page SHOULD include the name and organisation of the recipient. If necessary, the fax cover page SHOULD be customised for each outgoing fax.

NET.4.3.A8 Appropriate Disposal of Consumable Fax Accessories and Spare Parts

All fax consumables from which information on sent and received fax messages might be derived SHOULD be destroyed before disposal or disposed of by a reliable specialised company. The same procedure SHOULD also be followed for replaced parts that contain information. Maintenance companies that service or repair fax machines SHOULD be required to handle them appropriately. Regular checks SHOULD be carried out to determine whether the rules established on handling are being followed.

NET.4.3.A9 Using Transmission and Reception Logs [Chief Information Security Officer (CISO)]

The transmission processes of incoming and outgoing faxes SHOULD be logged. The communication journals available on standard fax machines SHOULD be used for this. If the fax ma-

chines have logging functions, they SHOULD be activated. Logging SHOULD be activated for fax servers. A decision SHOULD be made regarding the information that should be logged.

The communication journals and log files of fax machines SHOULD be regularly evaluated and archived. They SHOULD undergo random inspections for irregularities. Unauthorised persons SHOULD not be able to access the communication journals or the logged information.

NET.4.3.A10 Control of Programmable Destination Addresses, Logs and Distribution Lists

Programmable speed dial keys or destination address memories SHOULD be checked regularly to see if the desired numbers match the respective programmed numbers. Fax numbers that are no longer required SHOULD be deleted. Appropriate documentation SHOULD be created when a new entry is added or a target number is changed.

Requirements in Case of Increased Protection Needs

Generic suggestions for module NET.4.3 *Fax Machines and Fax Servers* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

NET.4.3.A11 Protecting Against Fax Machine Overload [IT Operation Department] (A)

Sufficient communication lines or channels SHOULD be available. The expected fax volume SHOULD be estimated for a fax server. Components which are capable of handling this volume SHOULD be selected. Logs of fax servers SHOULD be checked regularly in order to prevent bottlenecks caused by overloads in good time. Fax data that is no longer required SHOULD be promptly deleted from the fax server.

NET.4.3.A12 Blocking Specific Fax Recipient and Sender Numbers (CIA)

Unwanted fax addresses – for example, those of companies that advertise by fax – SHOULD be blocked or only certain phone numbers allowed.

NET.4.3.A13 Designating Authorised Fax Operators [User] (A)

A few employees who may access the fax machine SHOULD be selected. These employees SHOULD distribute incoming faxes to the recipients so that they do not need to access the fax machine. These employees SHOULD be taught how to use the device and how to implement the necessary security measures. Every authorised user SHOULD be informed about who may operate the fax machine and who the person in charge of the fax machine is.

NET.4.3.A14 Producing Copies of Incoming Fax Messages [User] (A)

Faxes printed on thermal paper that may be required for some time SHOULD be copied or scanned onto plain paper, as the colour fades faster on thermal paper and thus becomes unreadable. Copies or scanned faxes SHOULD be archived appropriately.

NET.4.3.A15 Announcing and Acknowledging Fax Messages [User] (CIA)

Important faxes SHOULD be announced to the recipient before they are sent. The documents to be announced in advance SHOULD be specified. Employees who wish to send sensitive fax documents SHOULD be instructed to have the recipient confirm full receipt. For important or unusual faxes, the recipient SHOULD have the sender confirm that the fax document origin-

ates from the correct sender and has not been falsified. A suitable form of communication (telephone, for example) SHOULD be selected to announce or confirm the fax documents.

Additional Information

Currently there is no additional information on threats and security measures for module NET.4.3 *Fax Machines and Fax Servers*.

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module NET.4.3 *Fax Machines and Fax Servers*:

- G 0.2 Unfavourable Climatic Conditions
- G 0.4 Pollution, Dust, Corrosion
- G 0.8 Failure or Disruption of the Power Supply
- G 0.14 Interception of Information / Espionage
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.22 Manipulation of Information
- G 0.27 Lack of Resources
- G 0.31 Incorrect Use or Administration of Devices and Systems

Elementary Threats Requirements	G 0.2	G 0.4	G 0.8	G 0.14	G 0.16	G 0.18	G 0.19	G 0.22	G 0.27	G 0.31
NET.4.3.A1	X	X		X	X	X				
NET.4.3.A2	X					X			X	X
NET.4.3.A3									X	X
NET.4.3.A4				X	X	X	X	X		X
NET.4.3.A5										X
NET.4.3.A6				X		X	X	X		
NET.4.3.A7						X				
NET.4.3.A8				X			X			
NET.4.3.A9				X						
NET.4.3.A10				X			X	X		
NET.4.3.A11				X			X	X		X
NET.4.3.A12			X							
NET.4.3.A13			X	X						
NET.4.3.A14									X	X
NET.4.3.A15					X					



INF.1: Generic Building

Description

Introduction

Buildings are the outer physical setting in which business processes are carried out. A building thus ensures the protection of the stationary workplaces, processed information, and established information technology it houses. Furthermore, the infrastructure installations of a building are often what make business processes and IT operations possible in the first place. This is why both the building itself (i.e. walls, ceilings, floors, roof, windows and doors) and all the infrastructure facilities and utilities it contains (such as electricity, water, gas, heating and cooling) should be considered.

This module is based on an example in which a building is used by one or more organisational units of an organisation. These units may also have differing security requirements. Furthermore, all considerations must include the fact that almost every building can and should be entered by persons not belonging to the organisation (citizens, customers, suppliers). If a building is used in such a way by various parties, the design and equipment of the building must match the use concept of the building. An optimal environment should be ensured for the persons working in the building. The entry of unauthorised persons should be prevented in areas where they may compromise security, and it should be possible to operate the technology installed in the building in a safe and efficient manner.

Objective

This module describes the requirements to be implemented in order to ensure optimal use of a building with regard to information security. The safeguards resulting from the requirements depend on the type and size of the organisation. Requirements from this module may also be applied to large properties including several buildings, or to the use of individual sections of buildings used by multiple entities.

Not in Scope

This module considers technical and non-technical security aspects when planning and using typical buildings for companies and public authorities. This includes consideration of the whole lifecycle of buildings, from the creation of requirement specifications to conceptual design, furnishings, usage, building alterations and eventually moving out.

The cabling in a building is examined separately in module INF.3 *Electrotechnical Cabling* and INF.4 *IT Cabling*, and special rooms such as server rooms or archive rooms are examined in the corresponding modules of the INF layer.

Threat Landscape

For module INF.1 *Generic Building*, the following specific threats and vulnerabilities are of particular importance:

Fire

Buildings and the people and facilities therein may sustain serious damage due to fire. Along with damage caused directly by the fire, subsequent damage must also be taken into consideration. The primary source of danger in case of a fire is the toxic smoke. Most personal injury suffered during a fire is caused by smoke inhalation. Smoke may cause serious damage to facilities and IT systems, as well.

For example, the PVC chlorine gases generated during combustion combine with the moisture and extinguishing water to form hydrochloric acid. If the resulting hydrochloric acid vapours are spread via the air conditioning system, sensitive electronic devices located in a part of the building far from the site of the fire may become damaged.

Lightning

Lightning is the most significant threat to a building and the information technology therein during a thunderstorm. A lightning strike can release current strengths of up to 200,000 amperes at voltages up to several hundred thousand volts. This enormous amount of electrical energy is released and dissipated within 50 to 100 microseconds. A lightning strike of this order of magnitude at a distance of approximately two kilometres will still cause voltage spikes in the electrical cables in the building that could lead to the destruction of sensitive electronic devices. The closer the lightning strike, the greater the indirect damage resulting from the strike.

If a building is hit directly by lightning, damage will be caused by the dynamic energy released by the lightning strike. This may lead to damage to the building structure (roof and façade), damage caused by subsequent fires, or damage to electrical devices due to overvoltage.

Water

Water may, for example, damage a building and its facilities from the outside due to rain, high water, or flooding, or from the inside due to defects in water pipes.

Elementary Damage and Natural Disasters

Depending on the site of a building, it may be exposed to the risks of elementary damage and natural disasters to different degrees. Causes for natural disasters may include seismic, climatic or volcanic phenomena such as earthquakes, flooding, landslides, tsunamis, avalanches and volcanic eruptions. Examples of extreme meteorological phenomena include thunderstorms, hurricanes, or cyclones.

Threats in the Vicinity

Buildings may be damaged or impaired regarding their use due to events in the immediate environment – directly, for example, by the release of toxic substances or indirectly by rescue work, road blocks or evacuations.

Unauthorised Access

If unauthorised persons are able to access a building or individual rooms, this may entail a variety of other security threats. Unauthorised persons may cause damage due to deliberate acts such as theft or manipulation of information or IT systems, but also to inadvertent misbehaviour (e.g. due to a lack of knowledge required, for example).

The goal of a break-in may be to steal IT components or other goods that are easy to sell, but it could also be to copy or manipulate data or IT systems. In this case, manipulations that are not so obvious can actually cause much more damage than direct acts of destruction. Property damage can also result from the unauthorised intrusion itself. If windows and doors are forced opened and damaged, they will need to be repaired or replaced.

Violation of Laws or Regulations

When erecting buildings, numerous laws and regulations must be taken into consideration – with regard to fire prevention or other aspects of structural security, for instance. While related violations may remain undetected for extended periods of time, they may have catastrophic effects, such as if firestops have not been installed in accordance with the applicable regulations.

Insufficient Firestops

Numerous cables and lines are routed through buildings that house IT operations. Fresh and waste water pipes, heating pipes, power supply cables and data transmission lines are some examples. It is impossible to prevent corresponding pipe and cable trays from crossing ceilings and firestops. When suitable firestops are not installed at such locations, fire and smoke may spread uncontrollably through them.

The highly dynamic nature of IT makes the continued expansion of networks necessary, even across firestops. The form in which this can be performed properly depends directly on the existing firestops and may vary greatly. If changes to a firestop are not carried out in accordance with the specifications of the respective firestop manufacturer, there is the risk that it may fail in the event of a fire and the fire may thus spread into the area protected by the firestop.

Failure of the Power Supply

In the event of a power failure, entire buildings or parts thereof may be rendered useless. It is not only the obvious, direct power consumers such as IT or lighting that depend on the power supply; today, all infrastructure facilities are directly or indirectly dependent on the power supply (e.g. lifts, air-conditioning technology, hazard alarm systems, security gates, automatic door locking systems, sprinkler systems, and private branch exchange systems). Even the water supply on floors above and below the ground depends on electricity due to the pumps required for pressure generation.

Requirements

The specific requirements of module INF.1 *Generic Building* are listed below. As a matter of principle, Building Services – that is, the organisational unit responsible for the infrastructure equipment in a building or property – is in charge of complying with the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the

implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Building Services
Further Roles	Chief Information Security Officer (CISO), Top Management, Construction Manager, Planner, Construction Company, Internal Services Department, Head of Organisation, Employee

Basic Requirements

For module INF.1 *Generic Building*, the following requirements **MUST** be implemented as a matter of priority:

INF.1.A1 Planning the Building Protection [Planner, Chief Information Security Officer (CISO)] (I)

The protection for the building **MUST** be defined based on the planned and existing use of a building and the protection needs of the business processes performed within it. Many different security aspects regarding the protection of persons, commodities and IT in the building must be taken into consideration, from fire prevention and electrical aspects to site access control. The security requirements from different areas **MUST** be coordinated.

INF.1.A2 Appropriate Segmentation of Circuits

It **MUST** be checked regularly whether the protection of the circuits and the circuit design still meet the actual requirements.

INF.1.A3 Compliance with Fire Prevention Regulations

The existing fire prevention regulations and the requirements imposed by the building inspectors **MUST** be met. The escape routes **MUST** be identified properly and kept unobstructed. The local fire brigade **SHOULD** be consulted when fire prevention plans are being developed. The fire prevention regulations derived from the building code are not sufficient for the fire prevention requirements of IT. As a consequence, an IT-related fire prevention concept **MUST** be drawn up and implemented.

Unnecessary fire loads **MUST** be avoided. This includes the regular disposal of waste paper and packaging waste.

There **MUST** be a Fire Safety Officer or another person familiar with the tasks involved who is also trained accordingly.

INF.1.A4 Fire Detection in Buildings [Planner]

Buildings **MUST** be equipped with a sufficient number of smoke detectors. In case of larger buildings, a fire alarm control panel (FACP) connected to all detectors **SHOULD** be implemented. If smoke is detected, an alert **MUST** be triggered that is sure to be noticed by all the persons located in the building. All smoke detectors and components of a fire alarm system **MUST** be checked regularly for functionality. It **MUST** be checked regularly that the escape routes are usable and not blocked by any obstacles so that the building can be evacuated quickly in the event of a dangerous situation.

INF.1.A5 Hand-Held Fire Extinguishers

A sufficient number of sufficiently dimensioned hand-held fire extinguishers with the fire class required in each case (based on DIN EN 3 Portable fire extinguishers) **MUST** be available for immediate firefighting measures. The hand-held fire extinguishers **MUST** be inspected and serviced regularly. The employees **SHOULD** be instructed regarding the use of the hand-held fire extinguishers.

INF.1.A6 Closed Windows and Doors [Employee]

Windows and doors facing the outside of a building (balconies, terraces) **MUST** be closed whenever the corresponding rooms are not in use. Corresponding instructions **MUST** be issued in this regard. It **MUST** be checked regularly whether the windows and doors are locked after everyone has left the room. Fire and smoke control doors **MAY NOT** be kept open for an extended period of time.

INF.1.A7 Site Access Regulations and Control [Head of Organisation]

Access to building parts and rooms requiring protection **MUST** be governed by a policy and controlled. There **SHOULD** be a concept for site access control. The number of persons with site access authorisation **SHOULD** be reduced to the bare minimum for every area. Additional persons **MAY** only be granted site access upon previous review of the necessity. The site access authorisations granted **SHOULD** be documented. The site access control safeguards **MUST** be checked regularly for effectiveness.

INF.1.A8 Smoking Ban [Employee]

Smoking **MUST** be prohibited in rooms containing IT or storage media (server rooms and storage media archives, but also document archives) where fires or contamination may lead to large amounts of damage. When establishing or tolerating smoking areas, it **MUST** be checked regularly that site access control is not bypassed in the process.

Standard Requirements

For module INF.1 *Generic Building*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

INF.1.A9 Security Concept for Building Use [Planner, Chief Information Security Officer (CISO)] (I)

There **SHOULD** be a security concept for building use. The security concept for the building **SHOULD** be adapted to the overall security concept of the organisation. It **SHOULD** be updated regularly.

Sensitive rooms or building areas **SHOULD NOT** be located in highly exposed or particularly hazardous areas.

INF.1.A10 Compliance with Relevant Standards and Regulations [Construction Company, Construction Manager]

When planning, erecting and converting buildings and installing technical equipment, all relevant standards and regulations **SHOULD** be taken into consideration.

INF.1.A11 Locked Doors [Employee]

Employees SHOULD be instructed to lock their offices or lock up their work documents when they are not in their offices. It SHOULD be checked sporadically whether this is being implemented.

INF.1.A12 Key Management

For all keys to the building (including for floors, hallways and rooms), a lock-up plan SHOULD be present. The manufacture, storage, management and issue of keys SHOULD be organised on a centralised basis. Backup keys SHOULD be available and secured, but kept at hand for emergencies. Keys not issued SHOULD be stored securely. Every key issued SHOULD be documented.

INF.1.A13 Regulations Governing Access to Distributors

Access to the distributors of all supply facilities within a building SHOULD be possible in short order in case of need. Access to distributors SHOULD be restricted to a small group of authorised persons.

INF.1.A14 Lightning Protection Devices

A lightning protection system SHOULD be installed according to the valid standard. A comprehensive lightning and overvoltage protection concept SHOULD be present. The lightning protection devices for buildings with comprehensive IT equipment SHOULD at least meet the protection class II according to DIN EN 62305, "Lightning protection". The lightning protection system SHOULD be inspected and serviced regularly.

INF.1.A15 Plans Detailing the Location of Supply Lines

Up-to-date layout plans of all supply lines SHOULD exist. It SHOULD be specified who is responsible for the layout plans of all supply lines, along with corresponding updates. The plans SHOULD be stored in such a way that only authorised persons may access them, but they must be quickly accessible in case of need.

INF.1.A16 Avoidance of References to the Locations of Sensitive Building Areas

Information on the locations of sensitive areas SHOULD be avoided. Sensitive areas of buildings SHOULD not be easily visible from the outside.

INF.1.A17 Structural Smoke Protection [Planner]

The structural smoke protection SHOULD be checked after installation and conversion work. The smoke protection components SHOULD be tested for functionality at regular intervals.

INF.1.A18 On-site Fire Prevention Inspections

On-site fire prevention inspections SHOULD be performed at regular intervals, or at least once or twice a year. Deficiencies identified during on-site fire prevention inspections SHOULD be rectified immediately.

INF.1.A19 Prompt Notification of the Fire Safety Officer

The Fire Safety Officer SHOULD be informed of work being performed on cable trays, hallways and escape and rescue routes. They SHOULD check that fire prevention safeguards are being implemented properly.

INF.1.A20 Alert Plan and Fire Drills

An alert plan for the measures to be taken in case of a fire SHOULD be drawn up. It SHOULD be updated periodically. Fire drills SHOULD be performed at regular intervals. The alert plan SHOULD be reviewed and updated at regular intervals.

Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.1 *Generic Building* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

INF.1.A21 Independent Electrical Supply Lines (A)

The IT SHOULD be supplied via two separate and independent supply lines.

INF.1.A22 Secure Doors and Windows (CIA)

Doors and windows SHOULD be selected on the basis of the security objectives of the area to be secured, the protection needs of the organisation and the appropriate classification in the relevant standards. All surrounding safeguarding measures via windows, doors and walls SHOULD be of equal quality and appropriate regarding burglary, fire and smoke. It SHOULD be checked regularly that the safety doors and windows function properly.

INF.1.A23 Formation of Security Zones [Planner] (C)

Rooms with similar protection needs SHOULD be consolidated into zones in order to treat comparable risks uniformly and be able to reduce the costs of required security safeguards. A security zone concept SHOULD be developed and documented for the building and property.

INF.1.A24 Automatic Drainage (A)

All areas endangered by water SHOULD be equipped with an automatic drainage system. The functionality of active and passive water drainage systems SHOULD be checked regularly.

INF.1.A25 Selection of Appropriate Locations [Top Management] (A)

When selecting or planning a building location, the environmental conditions that may influence information security SHOULD be checked. There SHOULD be an overview of the location-related threats. These threats SHOULD be addressed by means of additional compensating safeguards.

INF.1.A26 Gatekeeper or Security Service (CIA)

The tasks of the gatekeeper or security service SHOULD be documented unambiguously. The gatekeepers SHOULD observe and monitor all movements of persons at the gate and at all other entrances. All employees and visitors SHOULD identify themselves with the gatekeepers. Visitors SHOULD be escorted to the person to be visited or collected from the entrance. The gatekeepers SHOULD be promptly informed of any changes in site access authorisations.

INF.1.A27 Protection Against Breaking and Entering (CIA)

Adequate safeguards to prevent breaking and entering SHOULD be implemented that are adapted to the local conditions. The equality and consistency of the protection against breaking and entering during planning, implementation and operation SHOULD be assessed regularly

by a competent person. The employees SHOULD be aware of the regulations for protection against breaking and entering.

INF.1.A28 Air Conditioning for Human Beings (IA)

In larger buildings, the air supply SHOULD be ensured by air-conditioning (A/C) systems. The A/C systems SHOULD be designed in accordance with the actual use of the building. A/C systems SHOULD be serviced regularly.

INF.1.A29 Organisational Requirements Regarding Cleaning Contractors (CIA)

It SHOULD be checked whether the employees of the cleaning company contracted to clean the building use the keys and ID cards issued as stipulated in the contract. The cleaning staff SHOULD be adequately instructed regarding how IT is to be handled. The cleaning staff SHOULD be supervised when working in especially sensitive areas.

INF.1.A30 Selection of an Appropriate Building (CIA)

When selecting an appropriate building, it SHOULD be checked whether all security requirements relevant for later use can actually be implemented. For every building, the existing threats and the safeguards required to prevent or reduce damage SHOULD be documented in advance.

INF.1.A31 Moving Out of Buildings [Internal Services Department] (C)

Before moving out, an inventory of all items relevant for information security (hardware, software, storage media, files, documents, etc) SHOULD be created. After moving out, all rooms SHOULD be checked for items left behind.

INF.1.A32 Firestop Register (A)

A firestop register SHOULD be maintained. This SHOULD record all the individual types of such partitions. After work is performed on firestops, the changes SHOULD be entered into the register within four weeks.

INF.1.A33 Layout of Sensitive Building Areas (CIA)

Sensitive rooms or building areas SHOULD NOT be located in highly exposed or particularly hazardous areas. If sensitive rooms are located in exposed locations, sufficient safeguards SHOULD be implemented in order to secure them. This SHOULD be documented.

INF.1.A34 Intruder and Fire Detection System (A)

An intruder and fire detection system appropriate for the rooms and risks SHOULD be present. The intruder and fire detection system SHOULD be serviced and checked at regular intervals. It SHOULD be checked whether the recipients of intrusion and fire detection messages are capable of providing the appropriate reactions to the alarm from both a technical and personnel-related perspective.

Additional Information

For more information about threats and security safeguards for module INF.1 *Generic Building*, see the following publications, among others:

[27001A11]	ISO/IEC 27001:2013: Information technology - Security techniques - Information se-
------------	------------------------------------------------------------------------------------

	curity management systems - Requirements, especially Annex A, A.11 Physical and environmental security, International Organization of Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[ISFCF19]	The Standard of Good Practice for Information Security : Area CF19 Physical and Environmental Security, Information Security Forum (ISF), June 2018
[NIST80053P EP]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, especially Appendix F-PS Page F-2013, Family: Physical and environmental protection, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module INF.1 *Generic Building*:

- G 0.1 Fire
- G 0.2 Unfavourable Climatic Conditions
- G 0.3 Water
- G 0.4 Pollution, Dust, Corrosion
- G 0.5 Natural Disasters
- G 0.6 Catastrophes in the Vicinity
- G 0.7 Major Events in the Vicinity
- G 0.8 Failure or Disruption of the Power Supply
- G 0.10 Failure or Disruption of Supply Networks
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.29 Violation of Laws or Regulations
- G 0.34 Assault
- G 0.44 Unauthorised Entry to Premises

Elementary Threats Requirements	G 0.1	G 0.2	G 0.3	G 0.4	G 0.5	G 0.6	G 0.7	G 0.8	G 0.10	G 0.16	G 0.18	G 0.29	G 0.34	G 0.44
INF.1.A1	X	X	X	X	X	X	X	X	X		X	X	X	X
INF.1.A2								X						
INF.1.A3	X			X	X	X					X	X		
INF.1.A4	X										X	X		
INF.1.A5	X										X	X		
INF.1.A6			X				X			X				X
INF.1.A7							X			X				X
INF.1.A8	X			X										
INF.1.A9		X					X			X	X		X	X
INF.1.A10											X	X		
INF.1.A11										X				X
INF.1.A12	X		X							X	X			X
INF.1.A13								X	X					X
INF.1.A14	X				X			X	X		X			
INF.1.A15								X	X					
INF.1.A16													X	
INF.1.A17	X										X	X		
INF.1.A18	X			X							X	X		
INF.1.A19	X										X			
INF.1.A20	X				X	X							X	
INF.1.A21								X	X					

INF.1.A22	X						X			X			X	X
INF.1.A23							X			X			X	X
INF.1.A24			X		X									
INF.1.A25		X	X		X	X		X	X		X			
INF.1.A26										X				X
INF.1.A27										X				X
INF.1.A28		X												
INF.1.A29				X				X		X				X
INF.1.A30		X	X		X	X		X	X		X			X
INF.1.A31										X	X			X
INF.1.A32											X			
INF.1.A33										X				X
INF.1.A34	X													



INF.2: Data Centre/Server Room

Description

Introduction

Today, almost all strategic and operative functions and tasks are substantially supported by information technology (IT) or cannot even be executed without it. As a consequence, the requirements regarding the performance and availability of the IT systems and their connection to the network environment are constantly increasing. To meet these performance requirements, ensure that adequate reserve capacity is available and operate IT economically, public authorities and companies of all sizes concentrate their IT landscape in data centres.

A data centre is defined as follows:

1. If an organisation using IT has only one central area of IT operations, this, together with the required support areas, must generally always be treated as a data centre according to the protection needs. The term "area of IT operations" refers to rooms in which hardware is installed and operated to provide services and data. In addition to the area of IT operations, the data centre comprises all other technical support areas (power supply, supply of cold air, extinguishing technology, security technology, etc) that facilitate the correct operation and security of the area of IT operations.
2. If the organisation's IT operations are distributed over several areas within a building or the premises and these areas are connected among each other and to the IT users by internal LAN connections, the functionally most significant of these areas (at minimum) must be treated as a data centre. In addition, areas whose correct operation is crucial for 50% or more of the users or from which 50% or more of the services and data (proportionate to all areas) are provided must be treated as a data centre.
3. If the organisation using the IT is located at several physically separate sites and these are connected to each other by connections other than internal LAN connections, each of the sites must be considered and treated separately according to (1).
4. An area of IT operations in which IT required for critical business processes (processes whose disruption or failure would significantly impair the fulfilment of an organisation's primary tasks) is located must always be treated as a data centre, independent of the size or the proportion specified in number (2).
5. Areas of IT operations from which services for third parties are performed must always be treated as a data centre. Here, it is irrelevant whether these services are subject to fees.

6. If there is a justifiable interest to treat an area of IT operations (together with its support areas) as a server room contrary to the above regulations, reasons must be provided for the resulting reduction of security requirements.

If a data centre deviates from this definition, the area of IT operations under consideration is referred to as a server room. This definition is solely based on the significance of the IT structure for the fulfilment of tasks of the organisation using the IT structure and thus corresponds to the methodology according to DIN EN 50600.

If a server room is to be protected, the requirements in this module can be reduced accordingly. However, substantial and comprehensible reasons must be given for this (according to 6.) and the basic requirements must be implemented at minimum.

Objective

On the one hand, this module is directed towards organisations that operate a data centre and want to check if suitable security safeguards have been implemented in the framework of an audit. On the other hand, the module can also be used for estimating the security safeguards which have to be implemented if the IT in a data centre is to be centralised. The primary goal of the requirements described in this module is to maintain the secure operation of the data centre.

Not in Scope

This module is intended for mid-sized data centres only. The security requirements described here are not sufficient to protect high-security data centres such as those used in the banking sector. The main differences between high-security data centres and the medium-security data centres considered here relate to high availability, disaster tolerance, redundancy of components, resistance to elemental damage, energy efficiency and data security.

The present module is also not suitable for small information domains with, for example, only one or a very small number of servers or IT systems. An example for this is an SME with a small number of IT workstations and a server which is located in a separate room. In such cases it is often sufficient to implement module INF.6 *Storage Media Archives*.

To make the module easier to understand, technical details and planning variables were deliberately avoided. Further information can be found in the relevant standards, such as DIN EN 50600.

Threat Landscape

For module INF.2 *Data Centre/Server Room*, the following specific threats and vulnerabilities are of particular importance:

Incorrect Planning

If protection against elementary threats is not taken into account when designing a data centre, there is a very high risk of failure. For example, site risks such as air traffic, earthquakes, flooding or political issues may threaten the operational safety and availability. Massive impacts on the operation of a new data centre are also possible if the available bandwidth or the energy supply at the selected site is insufficient due to an incorrect conceptual design.

Unauthorised Site Access

If site access controls are lacking or insufficient, there is an increased risk that unauthorised persons may enter the data centre and cause unintentional (e.g. due to a lack of technical knowledge) or intentional damage. Attackers may thus, for example, extract sensitive data, steal or manipulate devices or manipulate servers. Insufficient site access controls thus have a particular impact on the availability, confidentiality and integrity of data or IT components.

Insufficient Monitoring

If the IT and infrastructure operated in the data centre is insufficiently monitored and supported, components may fail without being noticed. This may considerably impair the availability and the correct functioning of the data centre. In addition, failures are often less obvious. Without active monitoring, they may be noticed too late. When this occurs, it is often no longer possible to react in time.

Insufficient Air Conditioning in Data Centre

IT components require a specific operating temperature in order to function correctly. They also convert their energy into additional heat. If the air conditioning in a data centre is insufficient or non-existent, it will not be possible to keep the climatic conditions stable. If it is too cold or too hot, the devices may be operating outside their permissible temperature limits. The possible consequences include malfunctions or failures of technical components or damaged storage media.

Fire

If the fire prevention measures at a data centre are inadequate or non-existent, there is a risk that a fire may occur and spread rapidly. Fire and smoke may cause major damage. It may also not be possible to prevent the fire from reaching other areas in time.

Water

As a consequence of leaks in the data centre's infrastructure, flooding, burst pipes, defective sprinkler systems, canalisation damage or defects in the air conditioning system, water may enter the data centre. This may result in devices becoming damaged or no longer functioning. It could also trigger a short circuit that results in the total failure of the system, or even a fire.

Non-Existent or Insufficient Anti-Burglar Protection

Non-existent or inadequate anti-burglar protection makes it easy for unauthorised persons to enter a data centre. Offenders are thus able, for example, to steal or manipulate IT components or obtain confidential information. They may also destroy devices or damage the data centre in general.

Failure of the Power Supply

If the power fails and there is no redundant power supply, this can lead to significant operational disruptions of a data centre, and thus of the organisation. For example, in the event of a power failure, all IT services provided by the data centre will suddenly no longer be available. Data loss is also possible. A sudden loss of power may also cause damage to IT systems, active network components, telecommunication systems or monitoring technology.

Contamination

Dust and other contamination in a data centre may result in the loss of functionality of technical equipment. Contamination increases the rate of failure and wear of technical equipment.

Insufficient Route Dimensioning

If cables are not routed separately and minimum distances are not observed, this may cause malfunctions of the data centre's IT. Network expansions may also be problematic in that protection against fire and smoke may no longer be ensured. It must also be ensured that no more than 60% of the cross-section of cable routing openings in firewalls are filled with cables. The remaining 40% must be filled with fireproof mortar or another material approved for firewalls. If this regulation is not observed, it will be possible for a fire from an adjacent room to spread to the data centre.

Requirements

The specific requirements of module INF.2 *Data Centre/Server Room* are listed below. In general, is the responsibility of the Head of IT to fulfil the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of IT
Further Roles	Data Protection Officer, IT Operation Department, Planner, Maintenance Personnel, Employee, Building Services

Basic Requirements

For module INF.2 *Data Centre/Server Room*, the following requirements **MUST** be implemented as a matter of priority:

INF.2.A1 Definition of Requirements [IT Operation Department, Planner, Building Services] (I)

Adequate technical and organisational requirements **MUST** be defined and implemented for a data centre.

When planning a data centre or choosing suitable rooms, potential threats resulting from environmental impacts, as well as the security level of the IT components (in particular, availability), **MUST** also be taken into account. Moreover, protective safeguards against potential internal and external attacks **MUST** be considered when assessing the situation as a whole.

A data centre as a whole **MUST** be designed as a closed security area. In addition, it **MUST** have different security zones. To this end, administration, logistic, technical and IT areas **MUST** be clearly separated from each other. In the case of a server room, it **SHOULD** be checked whether it is possible to implement different security zones.

It **MUST** also be ensured that, where possible, supply lines (e.g. for water or gas) are not routed in the immediate vicinity of technical components requiring protection. Existing supply lines **MUST** be checked regularly for leaks, at least in the critical places.

INF.2.A2 Formation of Fire Zones [Planner]

Suitable fire zones for the rooms of a data centre **MUST** be defined. The security objective of a firewall or fire zone **MUST** be to protect not only the building and the people in it, but also its inventory and availability. Consequently, not only the spreading of a fire by flames and hot flue gases **MUST** be prevented; heat radiation and the spreading of cold smoke **MUST** also be blocked. In the case of a server room, it **SHOULD** be checked whether adequate fire zones can be implemented.

INF.2.A3 Use of an Uninterruptible Power Supply [Building Services]

An uninterruptible power supply (UPS) **MUST** be installed for all operationally relevant components of the data centre. As the power consumption of air conditioning systems is often too high for a UPS, the systems' control **MUST** be connected to the uninterruptible power supply at minimum. In the case of a server room, it **SHOULD** be checked whether operation of an UPS is necessary based on the availability requirements of the IT systems.

The UPS **MUST** be sufficiently dimensioned so that, in the event of a power failure, all components are supplied with power for a period long enough to ensure that no loss of data occurs.

In case of relevant changes, it **MUST** be checked whether the existing UPS systems are still sufficiently dimensioned. The battery of the UPS **MUST** be maintained within the required temperature range and preferably located in a separate area.

The UPS **MUST** be serviced and checked for functionality at regular intervals. In this context, the service intervals specified by the manufacturer **MUST** be observed (see *INF.2.A10 Inspection and Maintenance of Infrastructure*). In order to ensure that the UPS provides the required support time, the actual support time **MUST** be determined at regular intervals, and also every time changes to the consumers are made.

If IT devices are supplied via an UPS, they **MUST NOT** be connected to other IT devices via shielded cables.

INF.2.A4 Emergency Shutdown of the Power Supply [Building Services]

There **MUST** be suitable means to isolate the data centre from the power supply in case of an emergency. An emergency off switch, for example, **SHOULD** be installed for this purpose. A switch of this kind **MUST** not only disconnect the external power supply, but also switch off the entire UPS system. All emergency off switches **MUST** be protected such that they cannot be activated unintentionally.

INF.2.A5 Maintenance of Air Temperature and Humidity [Building Services]

In order to be able to reliably operate IT systems in accordance with the manufacturer's recommendations, it **MUST** be ensured that the air temperature and humidity in the area of IT operations is within the specified limits.

The actual thermal load in the cooled areas **MUST** be checked through calculation or measurement at regular intervals, as well as after any major changes.

If there is an air conditioning system, it **MUST** also be serviced regularly. If the temperature and humidity both deviate from the standard values, they **MUST** be recorded at intervals appropriate for the situation for a representative period of time.

INF.2.A6 Site Access Control [IT Operation Department, Building Services] (I)

Site access controls **MUST** be in place to prevent unauthorised access.

Site access controls adapted to the respective requirements **MUST** ensure that the organisation's own employees and temporary employees do not have access to IT systems outside of their area of responsibility.

It **MUST** also be ensured that visitors and external staff are individually registered by the site access controls and supervised during all work in the data centre.

Furthermore, all the possible ways to access a data centre **MUST** be monitored. The organisation's requirements regarding the site access control system **MUST** be documented in a concept with sufficient detail. In the case of a server room, it **SHOULD** be checked whether it is appropriate to monitor all site access options.

Moreover, it **MUST** be specified which internal and external persons are granted access for which period. In this respect, it **MUST** be ensured that no unnecessary or excessive access rights are granted. It **MUST** be checked at regular intervals whether the regulations regarding the use of site access controls are being observed.

INF.2.A7 Locking and Securing [Employee, Building Services]

All doors of the data centre **MUST** always be kept locked. Windows should already be avoided in the planning stage whenever possible. If there are windows, they **MUST** always be kept locked, as well. Doors and windows **MUST** provide protection adequate for the security level at hand against attempted attacks and environmental impacts (e.g. fire and smoke). Here, it must be considered that the architectural design of all spatial partitioning elements **MUST** be equivalent in terms of security, particularly with regard to security zones.

INF.2.A8 Use of a Fire Alarm System [Planner]

A fire alarm system **MUST** be installed in a data centre. It **MUST** monitor all areas. All alarms of the fire alarm system **MUST** be forwarded in a suitable manner (see also INF.2.A13 *Planning and Installation of Alarm Systems*). The fire alarm system **MUST** be serviced at regular intervals. It **MUST** be ensured that no particular fire loads are present in rooms which are in the fire zone of the data centre.

INF.2.A9 Use of an Extinguishing or Fire Prevention System [Planner]

An extinguishing or fire prevention system in line with the state of the art **MUST** be installed in a data centre.

In server rooms, a sufficient number of properly sized hand-held fire extinguishers **SHOULD** be used for this purpose. The fire extinguishers **MUST** be mounted so that they are easy to access in case of a fire. Every extinguisher **MUST** be inspected and serviced at regular intervals to ensure its functionality in case of an emergency. All employees **MUST** be instructed in the use of the hand-held fire extinguishers.

INF.2.A10 Inspection and Maintenance of Infrastructure [Maintenance Personnel, IT Operation Department, Building Services]

At minimum, the recommended intervals and guidelines for inspection and maintenance (or those specified in standards) **MUST** be followed for all components of the technical infrastructure. In order to be able to determine when which work was carried out, inspections and maintenance work **MUST** be logged.

Cable and pipe openings in firewalls **MUST** be checked at regular intervals to ensure that the walls are intact and compliant with the standards. The results **MUST** be documented.

INF.2.A11 Automated Infrastructure Monitoring [IT Operation Department, Building Services]

All fault alarms in the infrastructure (e.g. leak monitoring, air conditioning, power and UPS system) **MUST** be monitored automatically and forwarded as soon as possible in a suitable manner, such as via a monitoring system.

In the case of a server room, IT and support devices that do not or only occasionally need to be operated by a person **SHOULD** be equipped with a remote indication of malfunctions. The responsible employees **MUST** be alarmed promptly.

Standard Requirements

For module INF.2 *Data Centre/Server Room*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

INF.2.A12 Design and Implementation of Data Centre Perimeter Protection [Planner, Building Services]

The security safeguards for perimeter protection **SHOULD** be equivalent to those of the security concept for the building and its surroundings. Depending on the protection needs defined for the data centre and on the premises, the perimeter protection **SHOULD** consist of the following components:

- a wall or fence around the property
- security safeguards against accidental trespassing (crossing the property line)
- security safeguards against deliberate trespassing without the use of force
- security safeguards against deliberate trespassing through the use of force
- open land security safeguards
- visual identification of people and vehicles

INF.2.A13 Planning and Installation of Alarm Systems [Planner]

A consistent protection concept **SHOULD** be developed for the building under consideration. Only then **SHOULD** it be planned which alarm systems are required and installed for which building areas of the data centre and how alarms are to be handled. The concept **SHOULD** always be adapted if the use of the building areas changes.

The installed alarm system SHOULD be suitable for the relevant area of application. The notifications of the alarm system SHOULD be transmitted to a alarm receiving centre under consideration of the applicable technical connection requirements. The alarm receiving centre SHOULD be available at all times and able to react appropriately to the alarms in terms of its technology and personnel. The design of the transmission route between the alarm system installed and the assistance centre SHOULD be redundant. All transmission routes SHOULD be tested at regular intervals.

INF.2.A14 Use of an Emergency Standby Power System [Planner, Building Services]

The power supply from the grid of a power supply company SHOULD be supplemented by an emergency standby power system (ESPS). The fuel supply of the ESPS SHOULD be checked regularly. In order to maintain the protective effect of an ESPS, maintenance SHOULD be performed regularly (see INF.2.A10 *Inspection and Maintenance of Infrastructure*). Load and functional tests, as well as test runs under load, SHOULD be conducted when performing maintenance.

INF.2.A15 Overvoltage Protection Devices [Planner, Building Services]

Based on the currently applicable standard, a lightning and overvoltage protection concept should be developed and implemented in accordance with the principle of energetic coordination (annex of DIN EN 62305-4). The energetic coordination of the overvoltage protection devices SHOULD be documented in a concept and approved.

Lightning and overvoltage protection devices SHOULD be checked periodically and after known incidents, and replaced if necessary. Regardless of the size and design of the overvoltage protection, it SHOULD be noted that comprehensive and continuous potential equalisation is required for all electrical equipment connected to the overvoltage protection circuit. When adding new equipment, consideration SHOULD be given to potential equalisation.

INF.2.A16 Air Conditioning in Data Centres [Building Services]

It SHOULD be ensured that suitable environmental conditions in terms of air temperature and air humidity (see INF.2.A5 *Maintenance of Air Temperature and Humidity*), fresh air levels and suspended particle content are created and maintained in the data centre. The air conditioning SHOULD be sufficiently dimensioned for the data centre. All relevant values SHOULD be constantly monitored. If a value deviates from the standard, an automatic alarm SHOULD be emitted.

In computer room areas, the air conditioning systems SHOULD be fail-safe whenever possible (e.g. based on the redundant design of components).

INF.2.A17 Early Fire Detection [Planner, Building Services]

In order to be able to detect fires in data centres at a very early stage, an early fire detection system SHOULD be installed.

To prevent incipient fires from spreading, the early fire detection system SHOULD initiate voltage disconnection. The monitoring areas of the early fire detection system and the areas subject to voltage disconnection SHOULD be designed in sufficient detail to ensure the right balance between fire protection and the availability of the data centre.

The system for early fire detection SHOULD conform to the current state of the art. It SHOULD also be operated in accordance with the manufacturer's instructions and maintained at regular intervals.

INF.2.A18 Protection Against Water Leaks [Building Services]

In areas containing IT devices with primary functions, the installation of water pipes SHOULD be avoided. For example, there SHOULD be no radiators in the data centre.

If water pipes (e.g. for cooling directly within the data centre) cannot be avoided, it SHOULD be ensured that water leaks are detected early and the effects are minimised. The water pipes SHOULD be regularly checked for leaks by means of visual inspection. Alarms from detection systems SHOULD be forwarded to responsible employees to enable them to react quickly based on reaction plans and up-to-date documentation (see *INF.2.A13 Planning and Installation of Alarm Systems*).

INF.2.A19 Functional Testing of Technical Infrastructure [Building Services]

The technical infrastructure of a data centre SHOULD be tested regularly (at least once or twice a year) and following system modifications and extensive repairs. The results SHOULD be documented. A realistic function test SHOULD be performed on entire reaction chains in particular.

INF.2.A20 Regular Updates of Infrastructure and Construction Plans [Planner]

Construction plans, route plans, wiring diagrams, escape route plans, fire brigade route maps, and so on SHOULD be updated immediately after each modification and if the infrastructure or security technology has been expanded. In addition, the employees SHOULD be informed accordingly. It SHOULD be checked that all relevant plans are still up to date and correct at least once every three years.

Requirements in Case of Increased Protection Needs

Generic suggestions for module *INF.2 Data Centre/Server Room* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

INF.2.A21 Alternate Data Centre (A)

A geographically separate alternate data centre SHOULD be established and used. The dimensions of the alternate data centre SHOULD be such that all of the organisation's processes can be maintained. It SHOULD also be always ready for use. All of the organisation's data SHOULD be mirrored to the alternate data centre on a regular basis.

INF.2.A22 Implementation of Dust Protection Measures [Building Services] (IA)

If an existing data centre is expanded, suitable dust protection measures SHOULD be defined, planned and implemented. Persons who are not involved in the construction work themselves SHOULD check the dust protection measures frequently to make sure they are working properly and the regulations on dust protection are being followed.

INF.2.A23 Secure Structuring of Data Centre Cabling [Building Services] (A)

Cable routes SHOULD be thoroughly planned and implemented. All cables SHOULD be protected against unwanted mechanical loads, manipulation, eavesdropping attempts and fire. Separate cables SHOULD be used for different network types (e.g. data networks, networks for alarm systems and power systems). If cables for different networks are routed together, it

SHOULD be ensured that mutual interference is minimised. In addition, an effort SHOULD be made to achieve redundant routing.

INF.2.A24 Use of Video Monitoring Systems [Planner, Building Services, Data Protection Officer] (IA)

The site access control and intrusion detection systems SHOULD be supplemented by video monitoring systems. To this end, the areas where video monitoring systems are appropriate SHOULD be identified.

A planned video monitoring system SHOULD be consistently integrated into the overall security concept. The Data Protection Officer SHOULD always be involved in the planning, design and potential evaluation of video recordings.

The central technical components required for a video monitoring system SHOULD be installed in a suitable environment and protected. The video monitoring system SHOULD be tested regularly to ensure it is working properly.

INF.2.A25 Redundant Design of Uninterruptible Power Supplies [Planner]

To ensure the availability of a data centre, the UPS systems should have a redundant design. In case of a power failure, it SHOULD be possible for all components required for proper operation of the data centre to be supplied with power until an alternative power source can be connected.

INF.2.A26 Redundant Design of Emergency Standby Power Systems (A)

In the case of increased protection needs, emergency standby power systems SHOULD have a redundant design. It SHOULD be ensured that these systems are also maintained regularly (see INF.2.A10 *Inspection and Maintenance of Infrastructure*).

INF.2.A27 Conducting Alarm and Fire Drills (CA)

Regular alarm and fire drills SHOULD be conducted with the employees of the organisation. They SHOULD be based on an alarm plan in which the measures to be taken are documented. The measures SHOULD be reviewed regularly to ensure they are still correct, up to date and feasible.

INF.2.A28 Use of Higher-Level Alarm Systems (IA)

For areas of data centres with increased protection needs, alarm systems of VDS class C SHOULD be used exclusively.

Additional Information

For more information about threats and security safeguards for module INF.2 *Data Centre/ Server Room*, see the following publications, among others:

[BKRZ]	Leitfaden Betriebssicheres Rechenzentrum [Guide to Reliable Data Centres] : Federal Association for Information Technology, Telecommunications and New Media (Bitkom), December 2013, http://www.bitkom.org/Bitkom/Publikationen/Betriebssicheres-Rechenzentrum.html , last accessed on 05.10.2018
[DIN50600-1]	DIN EN 50600-1:2013-05 Information technology - Data centre facilities and infra-

	structures - Part 1: General concepts, May 2013
[DIN62305-4]	DIN EN 62305-4:2011-10 Protection against lightning - Part 4: Electrical and electronic systems within structures (IEC 62305-4:2010), October 2011
[VdSPeri]	Security Manual Perimeter: VdS 3143:2012-09 (01), Gesamtverband der Deutschen Versicherungswirtschaft e.V. (GDV) (ed.), http://vds.de/fileadmin/vds_publicationen/vds_3143_web.pdf , September 2012, last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module INF.2 *Data Centre/Server Room*:

- G 0.5 Natural Disasters
- G 0.6 Catastrophes in the Vicinity
- G 0.4 Pollution, Dust, Corrosion
- G 0.2 Unfavourable Climatic Conditions
- G 0.3 Water
- G 0.1 Fire
- G 0.7 Major Events in the Vicinity
- G 0.8 Failure or Disruption of the Power Supply
- G 0.10 Failure or Disruption of Supply Networks
- G 0.11 Failure or Disruption of Service Providers
- G 0.15 Eavesdropping
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.24 Destruction of Devices or Storage Media
- G 0.25 Failure of Devices or Systems
- G 0.26 Malfunction of Devices or Systems
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.32 Misuse of Authorisation

G 0.33 Shortage of Personnel

G 0.34 Assault

G 0.41 Sabotage

G 0.44 Unauthorised Entry to Premises

Elementary Threats	G 0.5	G 0.6	G 0.4	G 0.2	G 0.3	G 0.1	G 0.7	G 0.8	G 0.10	G 0.11	G 0.15	G 0.16	G 0.24	G 0.25	G 0.26	G 0.29	G 0.30	G 0.31	G 0.32	G 0.33	G 0.34	G 0.41	G 0.44
INF.2.A1	X	X					X									X							
INF.2.A2						X		X	X				X	X									
INF.2.A3								X															
INF.2.A4	X					X		X					X		X								
INF.2.A5				X																			
INF.2.A6												X					X		X				X
INF.2.A7												X					X		X				X
INF.2.A8						X		X	X				X	X									
INF.2.A9						X		X	X				X	X									
INF.2.A10						X		X	X					X									
INF.2.A11									X				X		X			X					
INF.2.A12							X					X					X					X	X
INF.2.A13	X	X	X		X	X	X	X	X			X	X	X	X		X	X			X	X	X
INF.2.A14								X															
INF.2.A15						X								X									
INF.2.A16				X																			
INF.2.A17						X		X	X				X	X									

INF.2.A1 8																					
INF.2.A1 9							X	X					X	X							
INF.2.A2 0													X	X	X	X					
INF.2.A2 1	X	X					X	X	X	X									X		
INF.2.A2 2			X																		
INF.2.A2 3							X	X		X			X		X					X	
INF.2.A2 4										X				X	X					X	
INF.2.A2 5							X														
INF.2.A2 6							X														
INF.2.A2 7														X		X					
INF.2.A2 8	X	X	X		X	X	X	X	X		X	X	X	X		X	X		X	X	X



INF.3: Electrotechnical Cabling

Description

Introduction

The cabling of IT systems and other devices includes all cables and distributors in the building, from the feed point of the distribution network operator to the terminal points of the consumers.

The proper and standards-compliant installation of the cabling is the basis for secure IT operations.

Objective

The objective of this module is to protect all cabling against the disruption or malfunction of the power supply.

Not in Scope

The IT cabling used for communication between IT systems is addressed in a separate module (see module INF.4 *IT Cabling*).

Threat Landscape

For module INF.3 *Electrotechnical Cabling*, the following specific threats and vulnerabilities are of particular importance:

Burning Cables

When a cable catches fire, either by spontaneous ignition or exposure to flames, there can be a variety of consequences. Some of these consequences include short circuits, broken ground conductors, the emission of aggressive gases, fire or the development of smouldering fires. Burning cables often only cause a slight increase in the temperature while the fire is forming. This then creates a risk of significant amounts of "cold" smoke being generated before the smoke detectors mounted on the ceiling are triggered.

Inadequate Dimensioning of Electrotechnical Cabling

When planning workstations, server rooms or data centres, the mistake of basing them on the current requirements alone is frequently made. This approach fails to take account of the fact that: the capacity of the power supply system must be expanded due to new requirements, such as the use of additional servers. However, cabling can only be expanded to the extent per-

mitted by the existing cables installed and by the amount of space available for additional cables and distributors.

Insufficient Documentation on Electrotechnical Cabling

If the exact locations of some cables are not known because the documentation is inadequate, these cables could be damaged during construction work inside or outside the building. It cannot be assumed that all cables and lines in the installation zones were installed according to applicable standards. Insufficient documentation can also make it more difficult to test, service and repair cabling.

Inadequately Protected Distributors

Distributors of the power supply network are often freely accessible and kept unlocked in corridors and staircases. Any person can thus open these distributor boxes, manipulate them and possibly cause a power failure. In addition, such distributors can be an immediate hazard due to the possibility of coming in direct contact with live parts after removing the screw plug fuses and their bases. Open doors on distribution boxes can also obstruct traffic routes and cause pinching or crushing injuries due to the edges.

Cable Damage

The less protection afforded to cables during installation, the greater the risk of damage. Such damage does not necessarily result in the immediate failure of connections. It is also possible that unauthorised connections could be established accidentally – for example, when cable sheathing or insulation is damaged and thus no longer completely intact. Such damage does not necessarily occur intentionally; it can also occur unintentionally.

Voltage Fluctuations and Over-/Undervoltage

Fluctuations in the supply voltage can result in malfunctions and damage to the IT systems. Such fluctuations range from extremely short and minor incidents which have little or no effect on the IT systems to total failures or destructive overvoltages. The fluctuations can originate in any part of the electrical supply system, from the electrical power grid of the power company to the power circuit to which the corresponding devices are connected.

Use of Inadequate Power Outlet Strips

There are usually not enough fixed electrical outlets installed to operate all equipment required. Power outlet strips are then usually used to compensate for the lack of outlets. When they are of insufficient quality, power outlet strips are a dangerous ignition source, and therefore a significant fire hazard. When several small power strips are connected in series to provide enough outlets for all equipment, the risks due to insufficient cable cross-sections and overvoltage increase even more.

Requirements

The specific requirements of module INF.3 *Electrotechnical Cabling* are listed below. As a matter of principle, the Head of Building Services is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can also be other roles that have further re-

sponsibilities in implementing requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of Building Services
Further Roles	Head of IT

Basic Requirements

For module INF.3 *Electrotechnical Cabling*, the following requirements **MUST** be implemented as a matter of priority:

INF.3.A1 Selection of Appropriate Cable Types

When selecting cables, technical transmission requirements and the environment the cables will be routed through and operated in **MUST** be taken into account. When selecting electrical cables, the relevant standards and regulations **MUST** be taken into account. With respect to the environmental conditions, factors such as temperatures, cable routes, tensile forces when routing the cables, installation methods and possible sources of disruption **MUST** be taken into account.

INF.3.A2 Planning Cable Routing [Head of IT]

Cables, cable routes and cable trays **MUST** be dimensioned adequately from both a functional and a physical perspective before they are installed. In this respect, future electrical requirements **MUST** also be taken into account, along with the provision of sufficient space for possible technical expansions in cable channels and trays. When routing the IT and power cabling together in a tray, crosstalk **MUST** also be avoided between the individual cables. As a general rule, It **SHOULD** be ensured that the IT cabling is routed separately from the electrotechnical cabling. It **MUST** be ensured that identifiable sources of danger are avoided.

INF.3.A3 Proper Installation

Installation work on IT cabling **MUST** be carried out carefully by qualified experts. At the same time, all relevant standards **MUST** be observed. The critical criteria used to determine whether the cabling was installed properly **MUST** therefore be inspected in all phases by the customer. At the time the material is delivered, it **MUST** be inspected as to whether the right cables and connection components were delivered. When laying power cables, special care **MUST** be taken to ensure that no damage occurs during installation and that the cable routes are selected in such a way that the installed cables cannot be damaged by normal use of the building.

Standard Requirements

For module INF.3 *Electrotechnical Cabling*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

INF.3.A4 Analysis of Cabling Requirements

As a general rule, an analysis of the requirements that may affect the economic efficiency of the cabling installation and its ability to meet all current and future requirements **SHOULD** be carried out. It **SHOULD** first estimate the short-term planned use by the users in the organisation and take this as a basis for projecting how use will evolve over the long term.

INF.3.A5 Technical Approval of Cabling

The cabling SHOULD undergo an approval process. Approval SHOULD only be given after all tasks to be performed are completed, the person in charge has reported the measures for approval and the inspections by the client have not revealed any unacceptable defects. The approval date SHOULD be selected so that there is enough time in advance to prepare for the approval inspections. In addition to checking if the invoice is correct and the scope of the work has been completed, compliance with the different standards for the electrotechnical cabling MUST also be checked during the approval process. For the approval report, a checklist SHOULD be drawn up. The checklist SHOULD also contain items relating to general requirements for the operational rooms. The approval report MUST be signed in a legally binding manner by the participants and all persons in charge. The report SHOULD be part of the internal documentation of cabling.

INF.3.A6 Overvoltage Protection

Any electrical network SHOULD be protected against overvoltage. To achieve this, an overvoltage protection concept corresponding to the applicable standards MUST be drawn up. Emergency standby power systems and uninterruptible power supplies SHOULD be included in the concept.

INF.3.A7 Removal or Deactivation of Unneeded Cables

If power cables are no longer required, they SHOULD be removed properly and completely. Afterwards, the fire seals MUST be sealed properly. Cabling suitable for continued use with the existing technology as reserve capacity SHOULD be kept in operating condition. At minimum, such cables MUST be labelled accordingly at the end points. As a matter of principle, an overview of the cables no longer needed SHOULD be created, and this documentation SHOULD be used to determine which cables be deactivated or dismantled/removed. Then, the corresponding documentation MUST be updated.

INF.3.A8 Fire Prevention in Trays

Trays SHOULD have sufficient capacity as to avoid cable fires. Furthermore, the extent to which trays are filled SHOULD be checked at reasonable intervals after the installation work is completed.

INF.3.A9 Documentation and Labelling of Cabling

An organisation SHOULD ensure that it has internal and external documentation for its cabling. The internal documentation MUST contain documentation of all electrotechnical cabling including the relevant installation and operation. The internal documentation SHOULD be comprehensively produced and maintained in such a way that operations and future development are provided with the best possible support. The external cabling documentation SHOULD be as neutral as possible.

INF.3.A10 Neutral Documentation in Distributors

There SHOULD be documentation in every distributor that reflects the current terminal block and line assignments. This documentation SHOULD be kept as neutral as possible and MUST enable secure switching. Only existing and used connections SHOULD be listed in the documentation, in addition to accumulating spare lines. Unless explicitly required, no information regarding the use of the lines SHOULD be specified. All further information SHOULD be provided in review documentation.

INF.3.A11 Inspection of Electrical Installations and Connections

All electrical installations, distributors and duct boxes for the cabling SHOULD be visually inspected (using spot checks at minimum) at regular intervals. A functional check SHOULD be performed in addition to the purely visual inspection, unless a corresponding check has been performed within the scope of the DGUV-V3 inspection. All irregularities found during a visual inspection or functional check MUST immediately be documented and reported to the organisational units responsible. The responsible organisational units MUST verify and correct the identified irregularities.

INF.3.A12 Avoidance of Electrical Ignition Sources

The use of electrical appliances and equipment intended for private use SHOULD be clearly regulated within an organisation. All electrical appliances and equipment SHOULD be checked by an electrician and determined to be safe before they are used. The use of power strips SHOULD be avoided whenever possible. Extra power outlets SHOULD be added to existing channel systems or in properly mounted cable conduits.

Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.3 *Electrotechnical Cabling* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

INF.3.A13 Secondary Power Supply (A)

Measures for supplying emergency power SHOULD be implemented to supplement the primary supply of power from the grid of a power supply company when the availability requirements are high. For this, a sufficiently dimensioned central UPS and an emergency standby power system (ESPS) SHOULD be established for the areas to be protected. It SHOULD be examined whether or not redundant connections to the grid operator should be installed. The ESPS and UPS MUST be serviced regularly.

INF.3.A14 A-B Supply (A)

It SHOULD be checked whether a two-duct power supply, known as an A-B supply, should be established in addition to the normal single-duct power supply for important IT components. In this respect, it SHOULD be ensured that its proper functioning is permanently monitored by suitable technical equipment, such as building services management systems (BSMS).

INF.3.A15 Material Safeguarding of Cabling (A)

In rooms visited by the general public or in parts of buildings that cannot be easily monitored, consideration SHOULD be given to protecting lines and distributors against access by unauthorised persons. In any case, the number and the size of the locations where power supply facilities are accessible to unauthorised persons SHOULD be reduced to the minimum.

INF.3.A16 Use of Cabinet Systems (A)

To improve the operational security of electrical connections and distributors, these devices SHOULD be installed or mounted in cabinet systems.

The IT hardware SHOULD be housed in cabinet systems whenever possible. The depth and width of such cabinet systems SHOULD be sufficient for the space requirements and SHOULD be equipped (or retrofittable with) relevant additional systems at any time.

INF.3.A17 Fire Seal Register (A)

A fire seal register SHOULD be maintained. This SHOULD record all the individual types of such partitions. After performing work on fire seals, the changes SHOULD be entered into the register within four weeks.

Additional Information

For more information about threats and security safeguards for module INF.3 *Electrotechnical Cabling*, see the following publications, among others:

[BGVA3]	DGUV Vorschrift 3: Electrical Installations and Equipment Accident Prevention Regulation, Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege [Institution for statutory accident insurance and prevention in the health and welfare services] (BGW), May 2014, https://www.bgw-online.de/SharedDocs/Downloads/DE/Medientypen/DGUV_vorschrift-regel/DGUV-Vorschrift3_Unfallverhuetungsvorschrift-elekt-Anlagen-Betriebsmittel_Download.pdf?__blob=publicationFile , last accessed on 05.10.2018
[DIN4102]	DIN 4102:2016-05 Fire behaviour of building materials and building components:
[IEC60364]	DIN IEC60364 - Low-voltage electrical installations:
[IEC62305]	IEC 62305 Information sheet: Protection against lightning DIN EN 62305 / VE 01805-305:2006, VDE (ABB), October 2006, https://www.vde.com/resource/blob/936756/5b65d838e75e83f750bd8fa23bb620b1/merkblatt-blitzschutznormen-13-download-data.pdf , last accessed on 05.09.2018
[VDE100]	DIN VDE 0100: Erection of low voltage installations:
[VDE105]	DIN VDE 0105-100 – Operation of electrical installations:

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module INF.3 *Electrotechnical Cabling*:

G 0.1 Fire

G 0.8 Failure or Disruption of the Power Supply

G 0.12 Electromagnetic Interference

G 0.18 Poor Planning or Lack of Adaptation

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.41 Sabotage

Elementary Threats Requirements	G 0.1	G 0.8	G 0.12	G 0.18	G 0.25	G 0.26	G 0.27	G 0.41
INF.3.A1		X	X	X	X		X	X
INF.3.A2	X	X	X	X	X			
INF.3.A3		X	X	X	X		X	
INF.3.A4		X	X		X		X	X
INF.3.A5		X	X		X		X	
INF.3.A6		X	X	X				
INF.3.A7	X	X	X					
INF.3.A8	X	X	X					
INF.3.A9		X	X		X			
INF.3.A10		X	X		X			
INF.3.A11		X	X	X	X	X	X	
INF.3.A12	X	X	X					
INF.3.A13		X						X
INF.3.A14		X	X					
INF.3.A15		X	X					
INF.3.A16		X	X			X	X	
INF.3.A17	X							



INF.4: IT Cabling

Description

Introduction

IT cabling consists of all communication cables and passive components (terminal blocks, splice distributors, patch panels) that an institution operates itself. It is also the physical basis of the communication network in an institution. The IT cabling ranges from external network connection points (e.g. a connection of a telecommunications provider or a DSL connection of an Internet provider) to the connection points of network subscribers.

Objective

The objective of this module is to protect the IT cabling in such a way that communications via these connections cannot be tapped, manipulated or impaired.

Not in Scope

Active network components (routers, switches, etc) are not dealt with in this module. The subject of wireless networks and WLAN is also excluded. These subjects are addressed in separate modules in the IT-Grundschrift Compendium. In this module, IT cabling refers to the physical basis of a manufacturer- and application-independent communication network, i.e. a local area network (LAN). This module does not differentiate between IT cables for transporting data and PBX cables for telecommunication services.

Threat Landscape

For module INF.4 *IT Cabling*, the following specific threats and vulnerabilities are of particular importance:

Burning Cables

Burning cables can cause significant damage. Some of these consequences include short circuits, broken ground conductors, the emission of aggressive gases, fire or the development of smouldering fires. Burning cables often only cause a slight increase in the ambient temperature while the fire is developing. This then creates a risk of significant amounts of "cold" smoke being generated before the smoke detectors mounted on the ceiling are triggered.

Inadequate Network Dimensioning

If an IT network is not dimensioned adequately, this will lead to availability problems. When planning networks, trays, server rooms or data centres, the mistake of basing the functionality, capacity or technical security design on the current requirements is made quite frequently. The

fact that network capacity may need to be expanded due to new requirements or changes in technical standards, for example, can be overlooked. However, networks can only be expanded to the extent permitted by the existing cables installed and by the amount of space available for additional cables.

Insufficient Documentation on Cabling

If the exact locations of some cables are not known because the documentation is inadequate, these cables could be damaged during construction work inside or outside the building. It cannot be assumed that all cables and lines in the installation zones were installed according to applicable standards. Insufficient documentation can also make it more difficult to test, service and repair cables.

Unauthorised Cable Connections

When unauthorised cable connections are made between IT systems or other technical components, there is a risk of security problems or operational disruptions. Unauthorised access to networks, systems, information or applications can be gained through unauthorised cable connections of this kind, for example. Information could additionally or exclusively be transmitted to the wrong recipients due to unauthorised cable connections. The normal connection may be disrupted.

Cable Damage

The less protection afforded to cables during installation, the greater the risk of damage. Such damage does not necessarily result in the immediate failure of connections; they can also result in sporadic transmission errors that are difficult to detect. It is also possible that unauthorised connections could be established accidentally – for example, when cable sheathing or insulation is damaged and thus no longer completely intact. Such damage does not necessarily occur intentionally; it can also occur unintentionally.

Impairment of Lines

The transmission characteristics of cables transmitting electric signals can be adversely affected by electric and magnetic fields in their environment. Crosstalk is a special form of this impairment of lines. Here, the interference is generally not caused by the environment, but by currents and voltages of signals transmitted on an adjacent line.

Eavesdropping and Manipulation

Eavesdropping attacks are an information security risk that should not be ignored. Basically, there is no such thing as a cable impervious to eavesdropping. Cables only differ with regard to the effort eavesdropping requires. Whether a line is actually being tapped can only be determined using sophisticated instruments. In addition to eavesdropping, other deliberate manipulations (or even the destruction of IT lines) pose a threat to the organisation. Line malfunctions can be caused deliberately and with manipulative intentions. Such manipulations often aim to disrupt IT operations or cause financial damage to the organisation.

Requirements

The specific requirements of module INF.4 *IT Cabling* are listed below. As a matter of principle, the Head of IT is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. There can be additional roles

with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of IT
Further Roles	Head of Building Services

Basic Requirements

For module INF.4 *IT Cabling*, the following requirements **MUST** be implemented as a matter of priority:

INF.4.A1 Selection of Appropriate Cable Types [Head of Building Services] (I)

When selecting cables, technical transmission requirements and the environment the cables will be routed through and operated in **MUST** be taken into account. In terms of communications technology, the selection of the cables **MUST** be determined by the required transmission rate and the distances between the transmission units. With respect to the environmental conditions, factors such as temperatures, cable routes, tensile forces when routing the cables, installation methods and possible sources of disruptions **MUST** be taken into account. Furthermore, the applicable standards and regulations **MUST** be taken into consideration when selecting the cables.

INF.4.A2 Planning Cable Routing [Head of Building Services]

Cables, cable routes and cable trays **MUST** be dimensioned adequately from both a technical and a physical perspective before they are installed. In this respect, future technical transmission requirements **MUST** be taken into account, along with sufficient space for possible technical expansions in cable channels and trays. When routing the IT and power cabling together in a tray, crosstalk **MUST** also be avoided between the individual cables. It **MUST** be ensured that identifiable sources of danger are avoided.

INF.4.A3 Proper Installation [Head of Building Services]

Installation work on the IT cabling **MUST** be carried out carefully by qualified experts. At the same time, all relevant standards **MUST** be observed. The critical criteria used to determine whether the IT cabling was installed properly **MUST** be inspected in all phases by the customer. At the time the material is delivered, it **MUST** be inspected as to whether the right cables and connection components were delivered. When laying IT cabling, special care **MUST** be taken to ensure that no damage occurs during installation and that the cable routes are selected in such a way that the installed cables cannot be damaged by normal use of the building. In addition, it **MUST** be ensured in general that the IT cabling is routed separately from the electrical cabling.

Standard Requirements

For module INF.4 *IT Cabling*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

INF.4.A4 Requirements Analysis for IT cabling

As a general rule, an analysis of the requirements that may affect the economic efficiency of the IT cabling installation and its ability to meet all current and future requirements **SHOULD** be carried out. In this analysis, the planned usage by the users in the organisation in the short

term SHOULD be estimated first and taken as a basis for projecting how IT usage will evolve over the long term. Furthermore, the security objectives of availability, integrity and confidentiality MUST also be taken into consideration in the requirements analysis for the IT cabling.

INF.4.A5 Technical Approval of IT Cabling [Head of Building Services] (I)

The IT cabling SHOULD undergo an approval process. This approval SHOULD only be granted after all tasks to be performed are completed, the person responsible for execution has reported the measure for approval, and the inspections by the customer have not revealed any unacceptable defects. The approval date SHOULD be selected so that there is enough time in advance to prepare for the approval inspections. During the approval process, information security aspects MUST be checked. For the approval report, a checklist SHOULD be drawn up. The checklist SHOULD also contain items relating to general requirements for the operational rooms. The approval report MUST be signed by the participants and all persons in charge.

INF.4.A6 Ongoing Updates and Revisions of Network Documentation

Documentation of the IT cabling SHOULD be considered an elementary part of all changes to the network and must be handled accordingly. In this respect, it SHOULD be possible to easily determine and modify all areas of the documentation affected by a given change. Furthermore, it SHOULD be examined whether the use of a document management system is advisable for the network documentation.

INF.4.A7 Removal or Deactivation of Unneeded IT Cabling [Head of Building Services]

If IT cabling is no longer required, it SHOULD be removed properly and completely. IT cabling suitable for continued use with the existing technology as reserve capacity SHOULD be kept in operating condition. An overview of the cables no longer needed SHOULD always be created and this documentation SHOULD be used to determine which cables should be deactivated or dismantled/removed. Finally, the documentation containing the inventory of IT cabling MUST be updated.

INF.4.A8 Fire Protection for Trays [Head of Building Services]

In order to avoid burning cables, trays SHOULD be equipped with sufficient ventilation. The fire protection regulations MUST be observed. Furthermore, the fire protection measures SHOULD be inspected at regular intervals after the installation work is completed.

INF.4.A9 Documentation and Labelling of IT Cabling

An organisation SHOULD ensure that it has internal and external documentation for its IT cabling. The internal documentation MUST contain all drawings relating to the installation and operation of the IT cabling. The internal documentation SHOULD be comprehensively produced and maintained in such a way that operations and future development of the IT networks are provided with the best possible support. There SHOULD be as little external documentation of the cabling as possible.

INF.4.A10 Neutral documentation in Distributors

There SHOULD be documentation in every distributor that reflects the current terminal block and line assignments. This documentation SHOULD be kept as neutral as possible. Only existing and used connections SHOULD be listed in the documentation. Unless explicitly required, no information regarding the use of the lines SHOULD be specified. All further information MUST be provided in audit documentation.

INF.4.A11 Monitoring of Existing Connections

All distributors and duct boxes for the cabling SHOULD be visually inspected (using spot checks at minimum) at regular intervals. A functional check SHOULD be performed in addition to the purely visual inspection. All irregularities found during a visual inspection or functional check MUST immediately be documented and reported to the organisational units responsible.

Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.4 IT Cabling are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

INF.4.A12 Redundant Cabling (A)

It SHOULD be examined, at least for the most important buildings, whether redundant primary IT cabling should be installed on separate trays. It SHOULD also be examined whether or not redundant connections to IT or telecommunication providers should be installed. If the availability requirements are high or very high, consideration SHOULD be given to installing redundant secondary and tertiary cabling in the relevant buildings. In this respect, the secondary cabling SHOULD be routed through at least two cable chutes located in separate fire zones in the building. If redundant cabling is used, its proper functioning SHOULD be checked at regular intervals.

INF.4.A13 Material Safeguarding of IT Cabling (IA)

In rooms visited by the general public or in parts of buildings that cannot be easily monitored, lines and distributors SHOULD also be protected against access by unauthorised persons. In any case, the number of locations available for accessing the routed cable SHOULD be kept to a minimum, and the lengths of the cable connections to be protected against unauthorised access SHOULD be kept as short as possible.

INF.4.A14 Prevention of Transient Currents on Shielding (A)

The power supply of the IT components SHOULD be chosen in such a way that disruptions due to transient currents on the shielding of data lines are prevented. Depending on the network type, precautions SHOULD be taken to protect the IT components against external irradiation, emissions from the line and detection of transient currents.

INF.4.A15 Use of Cabinet Systems (IA)

To improve the operational safety of active and passive network components, these devices SHOULD be installed or mounted in cabinet systems.

Additional Information

For more information about threats and security safeguards for module INF.4 *IT Cabling*, see the following publications, among others:

[DIN4102]	DIN 4102:2016-05 Fire behaviour of building materials and building components:
-----------	--------------------------------------------------------------------------------

[DIN41494]	DIN 41494 Mechanical structures for electronic equipment:
[DIN50173]	DIN EN 50173 Information technology - Generic cabling systems:
[DIN 50174]	DIN EN 50174 Information technology - Cabling installation:
[DIN50310]	DIN EN 50310:2017-02 Telecommunications bonding networks for buildings and other structures: February 2017
[DIN 50346]	DIN EN 50346:2010-02 Information technology - Cabling installation - Testing of installed cabling: February 2010
[DIN60297]	DIN IEC 60297 Mechanical structures for electrical and electronic equipment:
[IEC60364]	DIN IEC60364 - Low-voltage electrical installations:
[IEEE8023]	IEEE8023: IEEE 802.3 Standards in Ethernet networks: CSMA/CD, Ethernet Working Group, http://www.ieee802.org/3/ , last accessed on 05.10.2018
[ISO11801]	ISO/IEC 11801:2002-09: Information technology - Generic cabling for customer premises, International Organization for Standardization (ed.), ISO/IEC JTC1, September 2002
[VDE100]	DIN VDE 0100: Erection of low voltage installations:

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module INF.4 *IT Cabling*:

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.9 Failure or Disruption of Communication Networks

G 0.12 Electromagnetic Interference

G 0.15 Eavesdropping

G 0.18 Poor Planning or Lack of Adaptation

G 0.20 Information or Products from an Unreliable Source

G 0.21 Manipulation with Hardware or Software

G 0.25 Failure of Devices or Systems

G 0.26 Malfunction of Devices or Systems

G 0.27 Lack of Resources

G 0.29 Violation of Laws or Regulations

G 0.37 Repudiation of Actions

G 0.41 Sabotage

Elementary Threats Requirements	G 0.1	G 0.2	G 0.9	G 0.12	G 0.15	G 0.18	G 0.20	G 0.21	G 0.25	G 0.26	G 0.27	G 0.29	G 0.37	G 0.41
INF.4.A1			X	X		X	X		X	X	X			
INF.4.A2	X	X	X	X		X		X	X	X		X		X
INF.4.A3	X		X		X			X	X	X		X	X	X
INF.4.A4	X		X						X	X				X
INF.4.A5		X				X	X	X	X	X	X	X		X
INF.4.A6	X							X	X	X		X	X	X
INF.4.A7						X							X	
INF.4.A8					X			X						
INF.4.A9					X	X							X	
INF.4.A10					X									
INF.4.A11			X	X				X	X	X				
INF.4.A12	X		X						X	X	X			X
INF.4.A13			X		X			X	X					X
INF.4.A14			X	X					X	X				
INF.4.A15					X			X	X					X



INF.6: Storage Media Archives

Description

Introduction

Storage media archives are closed rooms within an organisation that are used to store of all kinds of storage media. In addition to storage media used for digital information, this also includes paper documents, film and other media.

Objective

This module describes the typical threats and requirements regarding information security for a storage media archive. The aim is to protect the information stored on this and other types of media.

Not in Scope

This module deals with technical and non-technical security requirements for storage media archives. Recommendations for correct archiving are not dealt with in this module. Information on this can be found in module OPS.1.2.2 *Archiving*.

Within the IT-Grundschutz framework, no increased requirements are placed on archive rooms with regard to fire protection. The containers in which the storage media are kept can fulfil additional fire protection requirements.

Threat Landscape

For module INF.6 *Storage Media Archives*, the following specific threats and vulnerabilities are of particular importance:

Unacceptable Temperature and Humidity

Fluctuations in temperature or excessive humidity in areas where long-term digital storage media are kept can cause data errors and reduce the useful storage life of the media.

Non-existent or Insufficient Rules

If employees fail to close or lock the windows and doors after leaving the storage media archive, storage media or other information can be stolen. Sensitive information can be viewed or passed on by unauthorised persons. In general, employees should be provided with relevant rules to ensure that vulnerabilities cannot occur. However, the specification of rules alone does not ensure they will be followed, nor does it ensure trouble-free operations. Many problems also arise when rules are in place, but unknown.

Unauthorised Access to Rooms Requiring Protection

Where access controls are lacking or inadequate, unauthorised persons may enter the storage media archive and view, steal or manipulate sensitive information. This may affect the availability, confidentiality or integrity of the archived information. Even when no immediate damage is apparent, operations can still be disrupted if it is necessary to examine how such an incident was possible, whether or not damage occurred or whether data or devices were manipulated.

Theft

Since many storage media are very small, it is all the easier to put them into a bag unnoticed or make off with them by hiding them under clothing. If there are no other copies, the information stored on the stolen media will no longer be available. Furthermore, the persons who have taken the storage media can read and disclose confidential information, possibly resulting in further damage. In most cases these consequences are considerably more significant than the costs of replacing the stolen storage media.

Requirements

The specific requirements of module INF.6 *Storage Media Archives* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for fulfilling the requirements. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified regularly according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Planner, Head of Building Services, Employee, Fire Safety Officer, Building Services

Basic Requirements

For module INF.6 *Storage Media Archives*, the following requirements **MUST** be implemented as a matter of priority:

INF.6.A1 Hand-Held Fire Extinguishers [Fire Safety Officer, Building Services]

In case of fire, suitable hand-held fire extinguishers **MUST** be easily accessible in the storage media archive. These hand-held fire extinguishers **MUST** be inspected and serviced regularly. The employees **MUST** be instructed in the use of the hand-held fire extinguishers.

INF.6.A2 Access Regulations and Control [Planner, Employee, Head of Building Services]

The storage media archive **MUST ONLY** be accessible to authorised persons. Access **MUST** be reduced to a minimum number of employees. Therefore, access **MUST** be regulated and controlled. A concept **MUST** be developed for access control. The effectiveness of the access control measures this contains **SHOULD** be regularly reviewed. To make it more difficult to bypass the access control system (and ideally prevent this from occurring), the entire room envelope **MUST** have a mechanical resistance that satisfies the protection needs; under no circumstances should it be less than RC2 (in accordance with DIN EN 1627).

INF.6.A3 Protection Against Dust and Other Contamination [Employee]

It **MUST** be ensured that the media in the storage media archive are adequately protected against dust and dirt. The requirements for this **MUST** be analysed as early as the planning phase. A strict smoking ban **MUST** be observed in storage media archives.

INF.6.A4 Closed Windows and Locked Doors [Employee, Building Services]

Where possible, a storage media archive **SHOULD NOT** have windows. If there are windows, they **MUST** be closed when leaving the storage media archive. The door **MUST** also be locked when leaving the room. Fire and smoke doors **MUST** also be closed.

The corresponding specifications **MUST** be included in suitable instructions. These instructions **MUST** be known to all employees. They **SHOULD** also be obliged to follow them. In addition, checks **MUST** be carried out regularly on whether the windows and doors are closed or locked after everyone has left the room.

Standard Requirements

Along with the basic requirements, the following requirements correspond to the state-of-the-art technology for module INF.6 *Storage Media Archives*. They **SHOULD** be implemented as a matter of principle.

INF.6.A5 Using Protective Cabinets

The storage media and other media in storage media archives **SHOULD** be stored in suitable protective cabinets.

INF.6.A6 Avoidance of Water Pipes [Building Services]

Water pipes that do not serve the operating needs of the room **SHOULD** generally be avoided in storage media archives. If water pipes are laid through the storage media archive, they **SHOULD** be checked regularly for leaks. In addition, precautions **SHOULD** be taken to ensure that any water leaks will be detected at an early stage. A storage media archive with high availability requirements **SHOULD** have reaction plans that specify targeted actions for reporting leaks.

INF.6.A7 Compliance with Climatic Conditions [Building Services]

It **SHOULD** be ensured that the permissible maximum and minimum values for temperature and humidity, as well as the dust content of the air in the room, are observed in the storage media archive. The air temperature and humidity values **SHOULD** be recorded and documented several times a year for a period of one week. Any detected deviations from the target value **SHOULD** be corrected promptly. The air conditioning system used **SHOULD** be serviced regularly.

INF.6.A8 Secure Doors and Windows [Building Services]

Security safeguards such as windows, doors and walls **SHOULD** be appropriate and up to the task of dealing with burglary, fire and smoke. Depending on the protection needs, a suitable resistance class **SHOULD** be implemented in accordance with DIN EN 1627. The functionality of all security doors and windows **SHOULD** be checked regularly. The entire room envelope **SHOULD** have a mechanical resistance that meets the protection needs (at least RC3 in accordance with DIN EN 1627).

Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.6 *Storage Media Archives* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

INF.6.A9 Intruder and Fire Detection System [Building Services] (CIA)

An appropriate intruder and fire detection system SHOULD be set up in storage media archives. This intruder and fire detection system SHOULD be inspected and serviced regularly. It SHOULD be ensured that the recipients of alarm messages ARE able to react appropriately to them.

Additional Information

For more information about threats and security safeguards for module INF.6 *Storage Media Archives*, see the following publications, among others:

[DIN1627]	DIN EN 1627:2011-09 Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification: September 2011
-----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module INF.6 *Storage Media Archives*:

- G 0.1 Fire
- G 0.2 Unfavourable Climatic Conditions
- G 0.3 Water
- G 0.4 Pollution, Dust, Corrosion
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.19 Disclosure of Sensitive Information
- G 0.21 Manipulation with Hardware or Software
- G 0.24 Destruction of Devices or Storage Media
- G 0.32 Misuse of Authorisation
- G 0.44 Unauthorised Entry to Premises
- G 0.45 Data Loss
- G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.1	G 0.2	G 0.3	G 0.4	G 0.16	G 0.19	G 0.21	G 0.24	G 0.32	G 0.44	G 0.45	G 0.46
INF.6.A1	X									X		
INF.6.A2					X	X	X	X	X	X		X
INF.6.A3	X			X	X	X	X	X		X		X
INF.6.A4	X		X	X	X	X	X	X	X			X
INF.6.A5					X							
INF.6.A6			X								X	
INF.6.A7		X										
INF.6.A8	X		X		X	X	X	X	X	X		X
INF.6.A9	X		X							X		



INF.7: Office Workplace

Description

Introduction

An office room is the area within an organisation where one or several employees are located in order to perform their tasks. This module describes the typical threats and requirements regarding information security for an office room.

Objective

The aim of the module is to protect information processed in office rooms.

Not in Scope

This module deals with technical and non-technical security requirements for office rooms. This module does not deal with recommendations on how to configure and safeguard the IT systems in such rooms. Information on this is included in SYS.2.1 *General Client* as well as in the operating-system-specific modules.

Cabling of office rooms is not addressed. For this, the modules INF.3 *Electrotechnical Cabling* and INF.4 *IT Cabling* must be considered separately. Requirements on fire protection and entry regulations for buildings are included in module INF.1 *Generic Building*. This module does not cover the requirements of an organisation either; information on this can be found in module ORP.1 *Organisation*.

Threat Landscape

For module INF.7 *Office Workplace*, the following specific threats and vulnerabilities are of particular importance:

Unauthorised Access

If site access controls are lacking or insufficient, unauthorised persons may enter an office room and extract sensitive data or steal or manipulate devices. This may affect availability, confidentiality or integrity of devices and information. Even when there is apparently no immediate damage, operations can still be disrupted if it is necessary to examine how such an event was possible, or whether or not damage occurred or data or devices were manipulated.

Impairment Due to Unfavourable Working Conditions

An office room not designed in accordance with ergonomic aspects or an unfavourable working environment may prevent employees from working undisturbed or using the employed IT

(or result in less than optimal use). The disturbances range from noise or high customer traffic to unfavourable lighting and poor ventilation. This limits working processes and results in insufficient usage of employee potential. Errors may also crop up during work, which can lead to a loss of data integrity.

Cleaning Staff, External Staff or Visitors

It is often more efficient to use the office room for small or short meetings. In such cases, visitors – as well as the cleaning staff and the external staff – may inspect internal information, threaten business processes and manipulate IT systems in various ways. These range from the improper handling of the technical equipment and attempts to "play" with the IT systems to the theft of documents or IT components. For example, cleaning staff may accidentally unplug a cable connection, water may leak into the IT or documents may be misplaced, or even disposed of along with the usual rubbish.

Manipulation or Destruction of IT, Accessories, Information and Software in the Office Room

For many reasons, attackers may try to manipulate or destroy IT systems, accessories and other storage media. The later such attacks are detected by the employee or the organisation, the greater the knowledge acquired by the perpetrators, the more far-reaching the impact on the corresponding work procedure, and the more effective the attacks will be. The manipulations range from unauthorised reading of the employee's sensitive data to the destruction of storage media or IT systems. This may result in significant downtime and process limitations.

Theft

As IT devices become ever more portable, it is growing easier to put them into one's pocket without being noticed. The theft of storage media, IT systems, accessories, software or data not only results in the expense of having to replace the equipment or restore it to working order, but also in losses resulting from a lack of availability. Furthermore, the person who steals the IT devices can read and disclose confidential information, which can result in further damage. In many cases, this is significantly more severe than the mere material loss of the device.

In addition to expensive IT systems, portable end devices which can be transported inconspicuously and easily are also often stolen. If the office rooms are not locked or monitored or the IT systems are not secured sufficiently, the equipment can be stolen quickly and inconspicuously.

Exposed Cables

Depending on the position of the connection points of the outlet sockets, the power supply and the data network in the office room, cables could be routed across the room, including across areas where people walk. Exposed cables like these not only constitute tripping hazards which may result in personal injury. If people trip over such cables, this may also damage IT devices.

Vandalism

Vandalism involves destroying or causing damage to someone else's property. The results are very similar to those of an attack, except that vandalism is not planned and executed like an attack and is usually the result of spontaneous, arbitrary destructiveness instead. Both external attackers (such as disappointed burglars) and internal attackers (such as frustrated or psycholo-

gically unstable employees) are potential perpetrators. Vandalism can be triggered by differences of opinion, personal problems, bullying or a poor work climate, among other reasons.

Requirements

The specific requirements of module INF.7 *Office Workplace* are listed below. As a matter of principle, the Chief Information Security Officer (CISO) is responsible for fulfilling the requirements. Furthermore, the CISO is responsible for ensuring that all requirements are fulfilled and verified according to the security concept defined. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Head of Building Services, Employee, Head of IT, Supervisor

Basic Requirements

For module INF.7 *Office Workplace*, the following requirements **MUST** be implemented as a matter of priority:

INF.7.A1 Suitable Selection and Use of an Office Workplace [Employee, Supervisor]

Rooms used as offices **MUST** be suitable for this purpose. The office rooms **MUST** be selected and equipped for the protection needs or the protection level of the information processed in such rooms. Therefore, office rooms used by the public **MUST** not be located in security-relevant areas. Germany's regulation on workplaces (*Arbeitsstättenverordnung*) **MUST** be implemented for the workplace and for the equipment of an office room.

INF.7.A2 Closed Windows and Locked Doors [Employee]

When employees leave their office rooms, all windows **MUST** be closed. If confidential information is located in the office room, the doors **SHOULD** be locked when leaving the room. This **SHOULD** be observed in particular in areas used by the public. The corresponding specifications **SHOULD** be included in suitable instructions. All employees **SHOULD** be required to implement the instructions. In addition, it **MUST** be checked regularly that the windows are closed when leaving the room and, if necessary, that the doors are locked. Furthermore, it **MUST** be ensured that fire doors and smoke control doors are actually closed.

Standard Requirements

For module INF.7 *Office Workplace*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

INF.7.A3 Exposed Cables

The power connections and access to the data network in the office room **SHOULD** be located near the IT devices. Cabling routed on top of the floor **SHOULD** be covered by a cable duct.

INF.7.A4 Site Access Regulations and Control

It SHOULD be ensured that unauthorised persons may not enter the office rooms. For this, a security concept SHOULD be drawn up and implemented. In addition, it SHOULD be checked regularly that the implemented safeguards are effective.

INF.7.A5 Ergonomic Workplace [Head of Building Services]

The workplaces of all employees SHOULD be ergonomic. Above all, the monitors SHOULD be positioned so that ergonomic and undisturbed working is possible. Here, it SHOULD be ensured that screens are not exposed to unauthorised persons. Germany's occupational protection ordinance for working at screens (*Bildschirmarbeitsschutzverordnung*, *BildscharbV*) SHOULD be implemented. All workplaces SHOULD be individually adjustable to ensure problem-free IT operation.

INF.7.A6 Tidy Workplace [Employee]

All employees SHOULD be required to keep their workplaces tidy when they leave them. Users SHOULD ensure that unauthorised persons cannot gain access to IT applications or inspect confidential information. All employees SHOULD carefully check their workplaces and ensure that no confidential information is freely accessible. Supervisors SHOULD check workplaces sporadically for exposure of sensitive information.

INF.7.A7 Suitable Storage of Official Documents and Storage Media [Employee, Head of Building Services]

The employees SHOULD be instructed to store confidential documents and storage media in a locked manner when they are not in use. To this end, suitable containers SHOULD be provided in the office rooms or in the vicinity.

Requirement in Case of Increased Protection Needs

Generic suggestions for module INF.7 *Office Workplace* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

INF.7.A8 Use of Anti-Theft Devices [Employee, Head of IT] (CIA)

If access to the rooms cannot be limited in a suitable manner, anti-theft protection devices SHOULD be used for all IT systems. In general, anti-theft protection devices SHOULD be used in areas frequented by the public.

Additional Information

For more information about threats and security safeguards for module INF.7 *Office Workplace*, see the following publications, among others:

[27001A12.2]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, especially Annex A, A.12.2 Protection from malware, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
--------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

[ArbStättV]	Workplaces Ordinance: Federal Ministry of Labour and Social Affairs (BMAS), http://www.bmas.de/DE/Service/Gesetze/arbeitsstaettenverordnung.html , last accessed on 05.10.2018
[BildscharbV]	Bildschirmarbeitsschutzverordnung (BildscharbV) [Occupational protection ordinance for working at screens]: https://www.arbeitsschutzgesetz.org/bildscharbv/ , last accessed on 05.10.2018
[DIN1627]	DIN EN 1627:2011-09 Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification: September 2011
[ISFCF19]	The Standard of Good Practice for Information Security : Area CF19 Physical and Environmental Security, Information Security Forum (ISF), June 2018
[NIST80053P EP]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, especially Appendix F-PS Page F-2013, Family: Physical and environmental protection, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module INF.7 *Office Workplace*:

G 0.2 Unfavourable Climatic Conditions

G 0.13 Interception of Compromising Interference Signals

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.21 Manipulation with Hardware or Software

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.44 Unauthorised Entry to Premises

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.2	G 0.13	G 0.14	G 0.15	G 0.16	G 0.18	G 0.21	G 0.22	G 0.23	G 0.24	G 0.30	G 0.44	G 0.46
INF.7.A1	X	X	X	X	X				X		X		
INF.7.A2		X		X			X	X	X	X	X	X	X
INF.7.A3					X								
INF.7.A4		X		X		X	X	X	X	X	X	X	X
INF.7.A5							X					X	
INF.7.A6		X					X					X	X
INF.7.A7		X	X	X		X	X	X				X	X
INF.7.A8				X									



INF.8: Working from Home

Description

Introduction

Teleworkers, freelance employees and the self-employed typically work from home. In contrast to a workplace in an office environment, the home workplace of an employee is located in the employee's living environment. Here, it must be possible to separate the occupational sphere sufficiently from the private sphere. If employees use home workplaces on an ongoing basis, various legal requirements must also be fulfilled; for example, the workplaces must meet the requirements regarding occupational health and ergonomics.

In case of a home workplace, it is not possible to assume the same infrastructural security as with the office rooms of an organisation; for example, the workplace is often also accessible for visitors or family members. That is why measures must be taken to achieve a security level that is comparable to an office room.

Objective

This module shows how the infrastructure of a home workplace can be established and operated in a secure manner. The core objective of the module is to protect the information of the organisation at the home workplace.

Not in Scope

The module contains basic requirements to be considered and fulfilled to counteract the threats specific to a home workplace. However, it only defines specific requirements for the infrastructure of a stationary workplace that can be accessed by third parties. Security requirements for the IT systems in use (e.g. computers) and in particular for the technical parts of teleworking (e.g. communication links) are not covered by the present module; they are described in OPS.1.2.4 *Teleworking* or in the relevant system-specific modules.

Threat Landscape

For module INF.8 *Working from Home*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Rules for Home Workplace

Since home workplaces are located outside of the organisation, the employees are mainly on their own in this environment. Non-existent or insufficient rules for the home workplace environment may result in IT problems and increased downtime. If IT problems cannot be solved through remote administration, an IT support technician may need to travel to the home

workplace in order to solve them. If the handling of internal and confidential information at the home workplace is not regulated in a transparent manner, employees may store the information in an incorrect manner. This may jeopardise the confidentiality and integrity of the information because it does not sufficiently prevent information from being accessed or modified without authorisation.

Unauthorised Access to Sensitive Rooms of the Home Workplace

Rooms of a home workplace in which sensitive information is stored and processed or sensitive devices are located are considered to be rooms requiring protection. If unauthorised persons may enter these rooms without being monitored, the confidentiality, integrity and availability of the data and information located there is significantly threatened.

Examples:

- An employee had set up an office at home in a separate room, but did not always lock the door. Once, while the children were briefly unsupervised, they began playing in the unlocked home office. The children then used important documents for colouring.
- When an employee was working on a project at his home workplace, he had an unexpected visitor. Whilst he was preparing coffee in the kitchen, the visitor briefly wanted to search for something on the Internet and accidentally infected the unlocked computer with malware.

Impairment of IT Usage of Adverse Working Conditions at the Home Workplace

A home workplace not designed in accordance with ergonomic aspects or an unfavourable working environment may make it impossible to work undisturbed or use the employed IT (or lead to less than optimal use). The disturbances range from noise or high customer traffic to unfavourable lighting and poor ventilation. This limits working processes and results in insufficient usage of employee potential. Errors may begin to crop up when working and cause a loss of data integrity.

Insecure Transport of Files and Storage Media

If documents, storage media or paper files are transported between the organisation and the home workplace, there is the risk that such information and data will be lost or stolen, or read or manipulated by unauthorised third parties. The transport of paper files and storage media may be insufficiently secured in many ways:

- If unique objects (meaning those without backups) are transported, losing them may make it impossible to fulfil targets and tasks as planned.
- If unencrypted storage media fall into the wrong hands, this may result in a serious loss of confidentiality.
- If sufficient access protection is not provided during transport, paper files and storage media can be copied or manipulated without this being detected.

Inadequate Disposal of Storage Media and Documents

If it is not possible for employees to dispose of storage media and documents properly at their home workplace, they may dispose of them in the household rubbish. Attackers may then use these items to obtain valuable information that can be used for targeted blackmailing at-

tempts or industrial espionage. The consequences include everything from a loss of knowledge to threats to the existence of the organisation, such as if important contracts cannot be concluded or partnerships fail as a result.

Manipulation or Destruction of IT, Accessories, Information and Software at the Home Workplace

The IT, accessories, information and software that are used at the home workplace can be manipulated or destroyed more easily than within the organisation. A home workplace is often accessible for customers, relatives and visitors of the family. Furthermore, it does not have the central protection measures of the organisation (e.g. gatekeeper services). If IT devices, accessories, information or software are manipulated or destroyed, the employee at the home workplace can often only work to a limited extent. Furthermore, it may be necessary to replace destroyed IT components, information and software solutions, which requires both financial and time resources.

Hazards Posed by Cleaning Staff or External Staff

Cleaning staff and external staff can pose a hazard to internal information, business processes and IT systems in various ways, ranging from the improper handling of technical equipment and attempts to “play” with the IT systems to the theft of documents or IT components. For example, cleaning staff may accidentally unplug a cable connection, water may leak into the IT or documents may be misplaced, or even taken out with the usual rubbish.

Higher Risk of Theft at the Home Workplace

The home workplace is usually not as secure as a workplace at a company or a public authority. Due to more elaborate precautions (e.g. security doors, gatekeeper service), the risk of someone entering the building without authorisation is much lower compared to a private home. In most cases, burglars primarily steal objects that can be sold quickly and easily. At the same time, IT used for work may also be stolen. However, the information on the stolen IT systems is often more valuable than the IT systems themselves. Burglars could attempt to make even more money through extortion or by transferring the data to a competitor than they could by selling the hardware.

Requirements

The specific requirements of module INF.8 *Working from Home* are listed below. As a matter of principle, the employee is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Employee
Further Roles	Chief Information Security Officer (CISO), Employee, Building Services

Basic Requirements

For module INF.8 *Working from Home*, the following requirements MUST be implemented as a matter of priority:

INF.8.A1 Securing Official Documents at the Home Workplace [Employee]

Official documents and storage media MUST be stored at the home workplace in such a way that they are inaccessible to unauthorised persons. Therefore, sufficient lockable containers (desks, wheeled containers, cabinets, etc) MUST be present. Every employee MUST leave their home workplace in a tidy condition and ensure that no sensitive information is freely accessible.

INF.8.A2 Transporting Working Material to the Home Workplace [Employee, Building Services]

The storage media and documents that can be processed at the home workplace and transported between the organisation and the home workplace (and vice versa) MUST be specified. In general, storage media and other documents MUST be transported securely. These rules MUST be communicated to all employees in a suitable manner.

INF.8.A3 Protection Against Unauthorised Access to the Home Workplace [Employee, Building Services]

The employees MUST be informed of the rules and safeguards to be considered with regard to anti-burglary and site access protection. For example, they MUST be instructed to close windows and lock doors when leaving the home workplace.

It MUST be ensured that unauthorised persons cannot enter the home workplace and cannot access official IT or documents at any time. Such measures MUST be checked at reasonable intervals, but at least in case of a change in circumstances at home.

Standard Requirements

For module INF.8 *Working from Home*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

INF.8.A4 Suitable Configuration of the Home Workplace [Employee, Building Services]

The home workplace SHOULD be separated from the private areas of the home based on a suitable room layout.

The home workplace SHOULD have suitable equipment that corresponds to the ergonomic requirements.

The home workplace SHOULD be also protected against burglary by suitable technical security safeguards. The security safeguards SHOULD be adapted to the local situation and the present protection needs.

INF.8.A5 Disposal of Confidential Information at the Home Workplace [Employee, Building Services]

Confidential information SHOULD be disposed of in a secure manner, meaning not just in the household rubbish. A special security policy SHOULD thus specify how to dispose of sensitive material. The required disposal facilities SHOULD be available.

Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.8 *Working from Home* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

INF.8.A6 Handling Official Documents with Increased Protection Needs at the Home Workplace [Chief Information Security Officer (CISO)] (CIA)

If employees must process official documents or information with increased protection needs, it SHOULD be considered whether working from home is feasible at all. Otherwise, the home workplace SHOULD be protected by extended high-quality technical safeguards.

Additional Information

For more information about threats and security safeguards for module INF.8 *Working from Home*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[DIN1627]	DIN EN 1627:2011-09 Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification: September 2011
[ISFBA23]	The Standard of Good Practice for Information Security : Area BA2.3 Protection of Databases, Information Security Forum (ISF), June 2018
[NIST80053]	Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, Revision 4, April 2013, http://nvlpubs.nist.gov/nist-pubs/SpecialPublications/NIST.SP.800-53r4.pdf , last accessed on 30.08.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module INF.8 *Working from Home*:

G 0.1 Fire

G 0.2 Unfavourable Climatic Conditions

G 0.3 Water

G 0.4 Pollution, Dust, Corrosion

G 0.13 Interception of Compromising Interference Signals

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.17 Loss of Devices, Storage Media and Documents

G 0.19 Disclosure of Sensitive Information

G 0.22 Manipulation of Information

G 0.23 Unauthorised Access to IT Systems

G 0.24 Destruction of Devices or Storage Media

G 0.30 Unauthorised Use or Administration of Devices and Systems

G 0.32 Misuse of Authorisation

G 0.41 Sabotage

G 0.44 Unauthorised Entry to Premises

Elementary Threats Requirements	G 0.1	G 0.2	G 0.3	G 0.4	G 0.1 3	G 0.1 4	G 0.1 5	G 0.1 6	G 0.1 7	G 0.1 9	G 0.2 2	G 0.2 3	G 0.2 4	G 0.3 0	G 0.3 2	G 0.4 1	G 0.4 4
INF.8.A1		X		X		X		X	X	X	X					X	
INF.8.A2						X		X	X	X	X						
INF.8.A3							X	X	X	X			X		X	X	X
INF.8.A4	X	X	X	X	X	X	X	X		X	X	X	X	X	X	X	X
INF.8.A5						X			X	X							
INF.8.A6	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X



INF.9: Mobile Workplace

Description

Introduction

Good network coverage and powerful IT devices such as laptops, smartphones or tablets make it possible for employees to work almost everywhere. Frequently, this means that official activities are not only performed in the rooms and buildings of the organisation, but at changing workplaces in various environments (e.g. hotel rooms, trains, or customer locations). The information processed in this way must be protected appropriately.

On the one hand, mobile working changes the duration, location and distribution of working times; on the other hand, it increases the requirements on information security because a secure IT infrastructure (as one finds in a typical office environment) cannot be expected for a mobile workplace environment.

Objective

This module describes security requirements for mobile workplaces. The aim is to create a security situation for such workplaces that is comparable to that of an office room.

Not in Scope

This module contains basic requirements to be considered and fulfilled if employees often work not only within the rooms of the organisation, but also at changing external workplaces.

Above all, it includes the organisational, technical and personnel requirements for fully or partially mobile work. In order to protect IT systems, storage media and documents used for mobile workplaces, all relevant modules such as *SYS.3.1 Laptops*, *SYS.3.2 General Smartphones and Tablets*, *SYS.3.4 Mobile Storage Media*, *NET.3.3 VPN*, *SYS.2.1 General Client*, and *INF.1 Generic Building* must be considered separately.

In addition, the security requirements for stationary display workstations set up by the employer (telecommuting workplaces) are not covered in the present module; they are described in *OPS.1.2.4 Teleworking*.

Threat Landscape

For module *INF.9 Mobile Workplace*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Rules for Mobile Workplaces

If mobile working is not regulated or only regulated insufficiently, the organisation may suffer financial damage or other consequences. For example, if it is not regulated which information can be transported and processed outside of the organisation and which protection measures must be considered, confidential information may fall into the wrong hands. Such information could be used by unauthorised persons to seriously disadvantage the organisation.

Degradation Due to a Changing Operational Environment

Since mobile storage media and end devices are used in a very wide range of environments, they are subject to a number of threats. These threats include, for example, damaging environmental conditions (such as extreme temperatures), as well as dust, moisture and transport damage.

In addition to such conditions, operational environments and their different security levels must be considered. In particular, smartphones, tablets, laptops and similar mobile end devices are not only portable, but can also communicate with other IT systems. Here, for example, malware can be transmitted or sensitive information can be copied. It may thus become impossible to fulfil tasks or visit customers, and IT systems may be damaged.

Manipulation or Destruction of IT Systems, Accessories, Information and Software at the Mobile Workplace

IT systems, accessories, information and software that are used in a mobile manner may be manipulated or destroyed more easily than when used within the organisation. The mobile workplace is often accessible to third parties. Furthermore, it does not have the organisation's central protection measures (e.g. gatekeeper services). If IT systems, accessories, information or software are manipulated or destroyed, the employee at the mobile workplace can often only work to a limited extent. Furthermore, it may be necessary to replace destroyed IT components or software solutions, which requires both financial and time resources.

Delays Caused by Temporarily Restricted Availability

In most cases, an employee at the mobile workplace does not have fixed working times and can be difficult to contact when on the move. This may delay the flow of information significantly. Even sending the information in an e-mail might not necessarily shorten the response time because it cannot be guaranteed that the mobile employee will read the e-mail promptly. Depending on the situation and organisation, temporarily limited availability has different effects, but may limit the availability of information significantly.

Insecure Transport of Files and Storage Media

If documents, storage media or paper files are transported between the organisation and the mobile workplaces, such information and data can be lost or stolen, or read or manipulated by unauthorised third parties. This may result in significant financial damage to the organisation. The transport of paper files and storage media may be insufficiently secured in many ways:

- If unique objects (meaning those without backups) are transported, losing them may make it impossible to fulfil targets and tasks as planned.
- If unencrypted storage media fall into the wrong hands, this may result in a serious loss of confidentiality.

- If sufficient access protection is not available during transport, paper files and storage media can be copied or manipulated without this being detected.

Inadequate Disposal of Storage Media and Documents

If it is not possible to dispose of storage media and documents properly, these items usually land in the household rubbish. When working in the field, employees also often throw drafts and other supposedly unnecessary documents into the nearest rubbish bin or just leave them at their hotel or on the train (for example). However, if storage media or documents are not disposed of properly, attackers may use them to obtain valuable information that can be used for targeted blackmailing attempts or industrial espionage. The consequences include everything from a loss of knowledge to threats to the existence of the organisation, such as if important contracts cannot be concluded or partnerships fail as a result.

Loss of Confidentiality of Sensitive Information

At mobile workplaces, it is easier for attackers to access confidential information stored on hard disks, removable storage media or on paper, particularly if they are professional attackers. They may also eavesdrop on communication links. If information is read or disclosed without authorisation, this will have serious consequences for the whole organisation. Among other things, a loss of confidentiality may result in the organisation infringing on laws or suffering from competitive disadvantages and financial damage.

Theft or Loss of Storage Media or Documents

The mobile workplace is generally not as secure as a workplace at a company or a public authority. Official IT devices and documents can thus be stolen more easily on a train, from a hotel room or even from the meeting rooms at customer locations.

In addition, IT systems or components can get lost. Alongside the purely material damage resulting from the immediate loss of the mobile device, the publication of sensitive data (e.g. e-mails, notes from meetings, addresses or other documents) can lead to additional (financial and/or reputational) damage.

Lack of Security Awareness and Carelessness in Handling Information

It can frequently be observed that there are a number of organisational regulations and technical security procedures for portable IT systems and mobile storage media available in organisations, but these measures are then undermined by careless handling of the specifications and technology. It is common to see mobile storage media left unattended in a meeting room during breaks or even in a train compartment, for example.

In addition, gifts in the form of storage media (e.g. USB pen drives) are sometimes accepted by employees and indiscriminately connected to their own laptops. Here, the laptop can be infected with malware that allows sensitive data to be stolen, manipulated or encrypted, and thus rendered temporarily unusable.

It is not unusual to observe people conducting open conversations about business-critical information on public transport or even during business meals. This can then easily be overheard by outsiders and potentially used to seriously disadvantage the employee or their organisation.

Requirements

The specific requirements of module INF.9 *Mobile Workplace* are listed below. As a matter of principle, the Chief Information Security Officer is responsible for fulfilling the requirements. Deviations from this are mentioned separately in the respective requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon.

Module Owner	Chief Information Security Officer (CISO)
Further Roles	Head of Personnel, Human Resources Department, Employee, User, Head of IT, Building Services, Supervisor

Basic Requirements

For module INF.9 *Mobile Workplace*, the following requirements **MUST** be implemented as a matter of priority:

INF.9.A1 Appropriate Selection and Usage of a Mobile Workplace [Supervisor, User]

The organisation **MUST** stipulate how employees are to select and use mobile workplaces in a suitable way. Characteristics that are desirable for a mobile workplace **MUST** be defined, along with criteria that rule out a mobile workplace. At minimum, the following **MUST** be specified:

- the workplace conditions that are allowed for processing sensitive information
- how employees at the mobile workplace should protect their information against unwanted third-party access
- when a permanent network and power supply is required
- the workplace environments that are absolutely forbidden

INF.9.A2 Rules for Mobile Workplaces [User, Head of IT]

For all work done when travelling, it **MUST** be specified which information may be transported and processed outside the company or public authority and which protective precautions must be taken. It **MUST** also be determined under which framework conditions employees with mobile IT systems may access internal information of their organisation.

Furthermore, there **MUST** be clear rules governing the transportation of IT components and storage media. For example, the IT systems and storage media that are allowed to be transported, the persons authorised to transport them and the basic security requirements to be considered **MUST** be specified. Records **MUST** be kept as to who has used which mobile devices at what times while not on the organisation's premises.

The users of mobile end devices **MUST** be made aware of the value of mobile IT systems and the information stored on them. They **MUST** be informed of the specific threats and safeguards regarding the devices they use. Moreover, they **MUST** be informed of the types of information

that may be processed on mobile IT systems. All users **MUST** be informed of the applicable rules to be followed, and they **MUST** be trained accordingly.

INF.9.A3 Site and Data Access Protection [Employee]

The employees **MUST** be informed of the rules and safeguards to be considered with regard to anti-burglary and site access protection at the mobile workplace. For example, they **MUST** be instructed to close windows and lock doors when leaving the mobile workplace (this is possible in case of hotel rooms, for instance). If this is not possible (e.g. on a train), the employees **MUST** store all documents and IT systems at a secure location when they are absent. It **MUST** be ensured that unauthorised persons cannot access official IT and documents at any time.

If rooms are left only for a short time, the clients in use **MUST** be locked or shut down so that they can only be used again after successful authentication.

INF.9.A4 Working with External IT Systems [Supervisor, User]

The organisation **MUST** specify how employees should work with external IT systems. Since the protection level of such IT systems may differ significantly from the security level of one's own organisation, every mobile employee **MUST** be informed of the risks involved in using external IT systems. The rules **MUST** specify whether and how sensitive information can be processed on external IT systems and the measures to prevent unauthorised persons accessing information. If employees work with external IT systems, it **MUST** be generally ensured that all temporary data created during such periods is deleted.

Standard Requirements

For module INF.9 *Mobile Workplace*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They **SHOULD** be implemented as a matter of principle.

INF.9.A5 Prompt Reporting of a Loss [Employee]

Employees **SHOULD** report any loss or theft of information, IT systems or storage media to their organisation immediately. To this end, there **SHOULD** be clear reporting channels and contact persons within the organisation.

INF.9.A6 Disposal of Confidential Information [Employee, Building Services]

Confidential information **SHOULD** be disposed of in a secure manner, meaning not just in the household rubbish. Before disposing of out-of-service or defective storage media and documents, they **MUST** be checked for sensitive information. If they contain sensitive information, the storage media and documents **MUST** be returned and disposed of and/or destroyed using the organisation's methods.

INF.9.A7 Legal Framework Conditions for Mobile Working [Head of Personnel, Human Resources Department]

Framework conditions regarding labour regulations and occupational safety laws **SHOULD** be observed and specified for mobile working. All relevant items **SHOULD** be clarified in employment agreements or in separate agreements between the mobile employee and employer as a supplement to the employment contract.

INF.9.A8 Security Policy for Mobile Workplaces [Head of IT]

All relevant security requirements for mobile workplaces SHOULD be documented in a security policy that is mandatory for the mobile employees. Furthermore, this policy SHOULD be adapted to the existing security policies of the organisation and agreed with all relevant departments. The security policy for mobile workplaces SHOULD be updated regularly. Moreover, it SHOULD specify that a substitute is to be appointed for each mobile employee and that the substitution process is to be practised regularly. The employees of the organisation SHOULD be made aware and trained with regard to the current security policy.

INF.9.A9 Encryption of Portable IT Systems and Storage Media [User]

In order to ensure that sensitive information cannot be seen by unauthorised third parties, employees SHOULD ensure that such information is secured in accordance with the internal policies. To this end, mobile storage media and clients SHOULD be encrypted. The cryptographic keys SHOULD be stored separately from the encrypted device.

Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.9 *Mobile Workplace* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security objectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

INF.9.A10 Using Anti-Theft Protection Devices (CIA)

If the IT system in use provides a means of anti-theft protection, this SHOULD be used. Anti-theft devices SHOULD always be used in places with increased public traffic or a high rate of user fluctuation. In this respect, the employees SHOULD always take into account that the protection of the information stored on the IT system usually has a higher value than the acquisition costs of the IT system. The acquisition and usage criteria for anti-theft devices SHOULD be adapted to the organisation's processes and documented.

INF.9.A11 Prohibiting Use of Insecure Environments (CIA)

The minimum criteria that working environments must fulfil to allow the mobile processing of information with increased protection needs SHOULD be determined. The criteria should cover the following topics at minimum:

- access and viewing by third parties
- closed and, if required, lockable or guarded rooms
- secured communication options
- a sufficient power supply

Additional Information

For more information about threats and security safeguards for module INF.9 *Mobile Workplace*, see the following publications, among others:

[27001A11.2]	ISO/IEC 27001:2013: Information technology - Security techniques - Information se-
--------------	------------------------------------------------------------------------------------

	curity management systems - Requirements, in particular Annex A, A.11.2 Equipment, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[27001A6.2.1]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, in particular Annex A, A.6.2.1 Mobile device policy, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[ISFPA2]	Standard of Good Practice for Information Security: Area PA2 Mobile Computing, Information Security Forum (ISF), June 2018
[NIST80046]	Guide to Enterprise Telework, Remote Access and Bring Your Own Device (BYOD) Security: NIST Special Publication 800-46, Revision 2, July 2016, http://dx.doi.org/10.6028/NIST.SP.800-46r2 , last accessed on 05.10.2018

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module INF.9 *Mobile Workplace*:

- G 0.14 Interception of Information / Espionage
- G 0.16 Theft of Devices, Storage Media and Documents
- G 0.17 Loss of Devices, Storage Media and Documents
- G 0.18 Poor Planning or Lack of Adaptation
- G 0.19 Disclosure of Sensitive Information
- G 0.21 Manipulation with Hardware or Software
- G 0.22 Manipulation of Information
- G 0.23 Unauthorised Access to IT Systems
- G 0.24 Destruction of Devices or Storage Media
- G 0.25 Failure of Devices or Systems
- G 0.29 Violation of Laws or Regulations
- G 0.30 Unauthorised Use or Administration of Devices and Systems
- G 0.31 Incorrect Use or Administration of Devices and Systems
- G 0.44 Unauthorised Entry to Premises
- G 0.45 Data Loss

G 0.46 Loss of Integrity of Sensitive Information

Elementary Threats Requirements	G 0.1 4	G 0.1 6	G 0.1 7	G 0.1 8	G 0.1 9	G 0.2 1	G 0.2 2	G 0.2 3	G 0.2 4	G 0.2 5	G 0.2 9	G 0.3 0	G 0.3 1	G 0.4 4	G 0.4 5	G 0.4 6
INF.9.A1	X	X		X	X	X	X			X						
INF.9.A2	X	X		X	X	X	X	X	X	X	X	X	X	X	X	
INF.9.A3	X	X			X	X	X		X			X		X		X
INF.9.A4					X		X					X	X			X
INF.9.A5	X				X											
INF.9.A6	X			X	X											X
INF.9.A7											X					
INF.9.A8	X			X	X	X	X	X			X	X	X			X
INF.9.A9	X	X	X		X		X									
INF.9.A10		X						X				X	X		X	
INF.9.A11	X				X					X	X					



INF.10: Meeting, Event, and Training Rooms

Description

Introduction

Every organisation usually has one or several rooms for holding meetings, training courses or other events. Specially equipped rooms are often designated for this purpose. Meeting, event and training rooms are predominantly characterised by the fact that they are used by different persons, groups or visitors and are generally only used for a limited period of time. IT systems that participants bring along are often operated together with the organisation's devices (e.g. external laptops connected to overhead projectors). These different usage scenarios result in a threat landscape that is more or less incomparable to the threat landscape of any other room.

Objective

The aim of this module is to protect the information processed in meeting, event and training rooms, along with the IT devices operated in such rooms. Moreover, it addresses the correct handling of visitors who use these rooms.

Not in Scope

This module addresses all technical and non-technical security aspects of using meeting, event and training rooms. Detailed recommendations on how to configure and protect the IT systems in such rooms are not addressed within the scope of this module; they are included in *SYS.2.1 General Client* and in the operating-system-specific system modules. Further aspects typical of meeting rooms, such as WLAN or video conference systems, are addressed in the modules of the layers *NET.2 Radio Networks* and *NET.4 Telecommunication*. The cabling in such rooms is addressed separately in the modules *INF.3 Cabling* and *INF.4 IT Cabling*. Fire prevention requirements are included in module *INF.1 Generic Building*.

Threat Landscape

For module *INF.10 Meeting, Event, and Training Rooms*, the following specific threats and vulnerabilities are of particular importance:

Non-Existent or Insufficient Rules

For example, if employees do not close the windows and doors after leaving the room or if confidential information is not removed from a whiteboard or flip chart, sensitive information may be obtained by unauthorised persons. In general, employees should be provided with rel-

evant rules so that corresponding vulnerabilities cannot occur. However, the specification of rules alone does not ensure they will be followed, nor does it ensure trouble-free operations. Many problems also arise when rules are in place, but unknown. In many cases, for example, the employees do not know that windows and doors must be closed after a meeting or how to correctly handle a used flip chart.

Incompatibility Between External and In-House IT Systems

IT systems are becoming more and more mobile and seeing increasing use in various environments. Mobile IT users often face scenarios where the IT systems cannot be used as planned due to incompatibility. For example, older devices do not have the same connectors and plugs as newer devices. Moreover, there are devices that require a corresponding adapter to interface with other devices. For example, if a corresponding adapter is not present, a laptop prepared with all the important data for a meeting cannot be connected to an overhead projector. Furthermore, attempts to connect the IT systems despite their incompatibility may damage the devices or the stored data.

Threats Caused by Visitors

It is not always easy to train and raise the awareness of employees regarding the proper handling of sensitive information and IT systems. In cases involving visitors, it cannot be assumed that they will handle the information and information technology according to the rules specified by the organisation they are visiting, especially since they do not know these rules in many cases. In general, visitors may obtain confidential information if the organisation's employees are careless. This can also be due to a lack of knowledge, as in the case of a visitor who mistakenly enters an employee's office when looking for the toilet and finds a whiteboard displaying confidential information. Visitors also may destroy or damage devices intentionally to obtain confidential information.

Exposed Cables

In meeting, event and training rooms, both the users and the type of room usage often change. This sometimes also requires permanent changes to the equipment, and therefore to the cabling in such rooms, as well. Depending on the positions of the connection points in the room (power and data outlets), cables could be routed temporarily across the room, including in areas where people walk. Tripping hazards like these not only threaten persons; IT devices can also be damaged if a person pulls on exposed cables when falling.

Theft

If the storage media (some of which are installed in a fixed location), IT systems, accessories, software or data installed in a meeting room are stolen, this will result in the expense of having to replace the equipment and restore it to working order. In addition, the meeting room will only be usable to a limited extent because the stolen items are missing. This may result in bottlenecks regarding the allocation of rooms. Furthermore, confidential information can be stolen, misused or forwarded.

In addition to expensive IT systems, portable end devices which can be transported inconspicuously and easily are often stolen. If the meeting, event and training rooms are not locked or monitored. If the IT systems are not secured sufficiently, the equipment can be stolen quickly and inconspicuously. This applies in particular if, for example, the rooms are not locked during meeting breaks.

Loss of Confidentiality of Sensitive Information

Confidential information can be disclosed via technical failure, carelessness, a lack of knowledge or deliberate acts. In such cases, the confidential information can be present in different locations, such as on storage media within computers (e.g. hard disks), on removable storage media (e.g. USB pen drives or optical media), in printed form on paper or on whiteboards or flip charts. If information is read or disclosed in an unauthorised manner, this may have serious consequences for the organisation (e.g. infringements of laws, competitive disadvantages, or financial damage).

Requirements

The specific requirements of module INF.10 *Meeting, Event, and Training Rooms* are listed below. As a matter of principle, the Head of Organisation is responsible for fulfilling the requirements. The Chief Information Security Officer (CISO) must always be involved in strategic decisions. Furthermore, the CISO is responsible for ensuring that all requirements are met and verified according to the security concept agreed upon. There can be additional roles with further responsibilities for the implementation of requirements. They are listed explicitly in square brackets in the header of the respective requirements.

Module Owner	Head of Organisation
Further Roles	IT Operation Department, Employee, Head of IT, Building Services

Basic Requirements

For module INF.10 *Meeting, Event, and Training Rooms*, the following requirements **MUST** be implemented as a matter of priority:

INF.10.A1 Secure Use of Meeting, Event and Training Rooms [Building Services, Head of IT]

The equipment present in the rooms **MUST** be protected appropriately against theft. Furthermore, the persons who are to administrate the IT and other systems present in the room **MUST** be defined. It **MUST** also be defined whether visitors may use IT systems they bring along and, if so, under which conditions. Furthermore, the network access points and telecommunications interfaces that can be accessed by visitors **MUST** be specified.

INF.10.A2 Monitoring of Visitors [Employee]

Visitors **MUST** be monitored outside of rooms that are expressly provided for visitors. Employees **MUST** be required to ensure that external persons are not left unsupervised.

INF.10.A3 Closed Windows and Doors [Employee]

The windows of the meeting, event and training rooms **MUST** be closed when leaving the rooms. For rooms that contain IT systems or sensitive information, the doors **MUST** be locked when leaving. In addition, it **MUST** be regularly checked that the windows and doors have been locked after leaving a room. Furthermore, it **MUST** be ensured that fire doors and smoke control doors are actually closed.

Standard Requirements

For module INF.10 *Meeting, Event, and Training Rooms*, the following requirements correspond to the state-of-the-art technology along with the basic requirements. They SHOULD be implemented as a matter of principle.

INF.10.A4 Planning Rooms for Meetings, Events and Training

When planning meeting, event and training rooms, the location of the rooms SHOULD be given special consideration. In particular, rooms often used by visitors SHOULD NOT be located close to parts of the building where confidential information is processed regularly. The level of confidentiality of the information discussed or processed in the rooms SHOULD be specified for each room.

INF.10.A5 Exposed Cables

The power connections SHOULD be located at the positions where overhead projectors, laptops or other appliances will be used in order to avoid exposed cables. In addition, cabling routed on top of the floor SHOULD be covered by a cable duct.

INF.10.A6 Configuring Secure Network Access [Head of IT]

It SHOULD be ensured that the IT systems visitors bring along cannot be connected to internal IT systems via the data network. Only IT systems expressly provided for this purpose SHOULD be able to access the LAN of the organisation. A data network for visitors SHOULD be kept separate from the LAN of the organisation. Network access points SHOULD be configured so that third parties are prevented from reading internal exchanges of data. Network connections in meeting, event or training rooms SHOULD be safeguarded. The IT systems in meeting, event and training rooms SHOULD be prevented from simultaneously establishing connections to the intranet and the Internet.

Furthermore, the power supply SHOULD be established separately from other rooms from the last sub-distributor.

INF.10.A7 Secure Configuration of Training and Presentation Computers [Head of IT]

Dedicated training and presentation computers SHOULD have a minimum configuration. The applications that can be used on the training and presentation computers during each event SHOULD be specified. The training and presentation computers SHOULD only be connected to a separate network that is isolated from the LAN of the organisation. Access to other networks SHOULD only be possible in a restricted manner.

INF.10.A8 Creating a Proof of Use for Rooms

Depending on the type of use of the meeting, event and training rooms, the persons using the rooms and the corresponding times of use SHOULD be evident. Proofs of use also SHOULD be provided for rooms where training with IT systems or particularly confidential meetings are held. It SHOULD be considered whether corresponding proofs of use should also be implemented for rooms that are accessible to every employee.

Requirements in Case of Increased Protection Needs

Generic suggestions for module INF.10 *Meeting, Event, and Training Rooms* are listed below for requirements which go beyond the standard level of protection. These SHOULD be taken into account IN THE EVENT OF INCREASED PROTECTION NEEDS. Final specification is performed within a risk analysis. The letters provided in brackets indicate which key security ob-

jectives are primarily addressed by the requirement (C = confidentiality, I = integrity, A = availability).

INF.10.A9 Resetting Training and Presentation Computers [IT Operation Department] (CA)

A procedure for resetting training and presentation computers to a pre-defined state after use SHOULD be specified. Changes made by users SHOULD be removed completely in such cases.

INF.10.A10 Ban on Carrying Mobile Phones (C)

Mobile phones SHOULD NOT be taken into confidential meetings and conversations. If necessary, this ban SHOULD be enforced by detectors.

Additional Information

For more information about threats and security safeguards for module INF.10 *Meeting, Event, and Training Rooms*, see the following publications, among others:

[27001]	ISO/IEC 27001:2013: Information technology - Security techniques - Information security management systems - Requirements, International Organization for Standardization (ed.), ISO/IEC JTC 1/SC 27, October 2013
[DIN1627]	DIN EN 1627:2011-09 Pedestrian doorsets, windows, curtain walling, grilles and shutters - Burglar resistance - Requirements and classification: September 2011

Appendix: Cross-Reference Table for Elementary Threats

The following Elementary Threats are relevant for module INF.10 *Meeting, Event, and Training Rooms*:

G 0.14 Interception of Information / Espionage

G 0.15 Eavesdropping

G 0.16 Theft of Devices, Storage Media and Documents

G 0.18 Poor Planning or Lack of Adaptation

G 0.21 Manipulation with Hardware or Software

G 0.24 Destruction of Devices or Storage Media

G 0.41 Sabotage

G 0.44 Unauthorised Entry to Premises

G 0.45 Data Loss

Elementary Threats Requirements	G 0.14	G 0.15	G 0.16	G 0.18	G 0.21	G 0.24	G 0.41	G 0.44	G 0.45
INF.10.A1			X		X	X		X	
INF.10.A2			X		X	X	X	X	
INF.10.A3					X	X	X	X	
INF.10.A4	X	X					X		
INF.10.A5				X					
INF.10.A6	X	X					X		
INF.10.A7	X			X	X		X		X
INF.10.A8							X	X	
INF.10.A9	X	X					X		
INF.10.A10	X	X							