Federal Office
for Information Security

Cloud
Computing

Cloud Computing Compliance Controls Catalogue (C5)

Criteria to assess the information security of cloud services

Table of Content

1 Introduction

1 Introduction

1.1 Current situation

Cloud computing is a new paradigm in ICT (information and communication technology). It consists of IT services being adjusted dynamically to the customer needs and made available through a network in a billable manner. These services are offered and used by means of technical interfaces and protocols. Moreover, the definition of cloud computing of the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik – BSI) (and the differentiation from IT outsourcing) applies as it is described on the BSI website[1].

Cloud computing is based on a high level of standardisation of the hard- and software as well as on the services build on it, details of which the customer is usually not very familiar with. As a consequence, a particularly high degree of trust in the cloud service provider is required, which has to be developed first.

A possible solution is combining the high standardisation of cloud computing with a high standardisation of information security. There is no lack of available information security standards in the context of cloud computing. Examples include the ISO/IEC 27001 and ISO/IEC 27017 standards, the rules of the CSA Cloud Controls Matrix and the BSI products like the IT-Grundschutz Catalogues and security profiles for software as a service (SaaS).

Among security experts and cloud service providers exists an informal consensus about the requirements that have to be met for secure cloud computing. A generally recognised requirements (or controls) catalogue on this, however, is not available yet.

There are different standards and certifications on the market which are used and maintained in parallel with great effort by many cloud providers. It is difficult for customers, however, to keep up an overview of the large number of different certifications. The present cloud computing compliance controls catalogue (hereafter referred to as “C5”) is intended to be an aid for the customer providing a better overview for a higher level of security and avoiding redundant audits.

1.2 Uniform requirements based on existing standards

The BSI uses C5 to present its current view of the mentioned informal consensus, and particularly to also facilitate an in-depth technical discussion. The requirements were, wherever possible, taken from known security standards and specified if necessary. They were supplemented by the BSI’s own requirements only to the extent needed. The origin of the requirements is documented in a transparent manner so that the cloud provider is able to easily perform a comparison with his own security level.

In cases considered appropriate, additional requirements were included in C5 for certain basic requirements. It’s BSI’s professional point of view that the basic requirements shall always be met for secure cloud computing. Moreover, it is up to the cloud customer to decide for their specific use case whether these basic requirements are sufficient or additional, optional requirements have to be met by the cloud provider. For this purpose, the additional requirements of C5 serve as a useful starting point.

It remains the challenge to prove the cloud customer that the requirements of C5 are fulfilled by means of a transparent audit performed by an independent, trusted third party. As for the basic requirements found in this catalogue, this audit

[1] https://www.bsi.bund.de/EN/Topics/CloudComputing/Basics/Basics_node.html

should build on existing standards and certifications and thus generate the lowest possible additional effort for the cloud provider.

C5 is therefore structured in such a way that it is suitable for an audit by a certified public auditor[2] according to an international auditing standard. This aims at an audit with comprehensive reporting with respect to the structure, procedures and organisation of safeguarding and monitoring measures (controls), especially including a statement concerning their design appropriateness and operational effectiveness.

Section 2 of this document referres to structure und content of C5. Information on the audit execution and reporting by an independent certified public auditor can be found in section 3. In section 3.6, application notes for potential cloud customers are listed. The requirements can be found in the sections 4 and 5. References to a selection of well-known standards are provided in a separate auxiliary document, which can be found on the BSI websites.

[2] The term “certified public auditor” is used in this document as a collective term and refers to people who did the specific examination for public accountants and hold that specific certificate in their country. In Germany, they are called “Wirtschaftsprüfer (WP)”, in USA they are called “certified public accountants (CPA)”. Using the country-specific terms is – by no means – meant to restrict audits against C5 to accountants of a specific country.

2 Structure and contents of C5

2 Structure and contents of C5

2.1 Structure of C5

Cloud services in terms of C5 are IT services which are made available to the customer by a service company (cloud provider, provider or service provider) over a network. Cloud services are offered, used and billed elastically and adapted to the requirements by defined technical interfaces and protocols. The range of the services offered within the cloud computing framework covers the entire spectrum of information technology and, among other things, includes infrastructure (e. g. computing power, storage), platforms and software.

C5 itself is subdivided into 17 sections (see section 2.2).

An objective is assigned to each section (see section 2.2). The objective provides the cloud provider a summarised target which they have to fulfill in the related section through corresponding organisational and operational measures and (procedural) organisation.

Individual requirements are assigned to each objective (see section 5). The requirements specify general principles, procedures and measures for fulfilling the objective. In this respect, a distinction is made between basic requirements and additional, optional requirements. The basic requirements are essential and the cloud provider has to meet and at least comply with as part of an audit according to this catalogue.

In addition to some basic requirements, additional, optional requirements are defined. They are classified as to whether especially confidentiality (C), availability (A) or both properties at the same time (C/A) are addressed with respect to the data processed in the cloud service. It turned out that there are no effective higher-level requirements for integrity (I) in addition to the basic requirements, which is why this category is missing here. The additional requirements are a starting point for requirements which the cloud customers could specify based on their individual use case.

The cloud provider is responsible for the design, description, implementation and effective operations of organizational and operational measures (controls) with which the requirements are implemented at the cloud provider. The entirety of the required measures is part of their internal control system concerning the cloud services. The design of this internal control system depends on the type of cloud service provided, the requirements of the cloud customers and the company goals of the cloud provider as well as on the associated specific risks.

A speciality in C5 are the so-called surrounding parameters for transparency which precede the requirements. Surrounding parameters for transparency address the transparency with respect to the general conditions according to which the cloud service is provided (e. g. the place of jurisdiction). By means of the information resulting from auditing these surrounding parameters for transparency, the customer can decide on the general suitability of the cloud service according to their internal targets.

2.2 Content-related presentation of the controls areas

Prior to the description of the detailed requirements in section 5, section 4 provides information on so- called “surrounding parameters for transparency”. They define the general framework for requests of information and are similar to the other requirements with regards to nomenclature and structure. The customers have to decide on the range of these parameters along their internal guidelines and policies.

C5 itself comprises of 17 sections (see table 1).

Section	Objective
Organisation of information security	Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organisation.
Security policies and work instructions	Providing policies and instructions with respect to the security claim and to support the business requirements.
Personnel	Making sure that employees, service providers and suppliers understand their tasks, are aware of their responsibility with regard to information security and that the assets of the organisation are protected if the tasks are modified or completed.
Asset management	Identifying the organisation's own assets and responsible persons as well as ensuring an appropriate level of protection.
Physical security	Preventing unauthorised physical access and protection against theft, damage, loss and failure of operations.
Operations	Assuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.
Identity and access management	Securing the authorisation and authentication of users of the cloud provider (usually privileged user) and the cloud customer in order to prevent unauthorised access.
Cryptography and key management	Using appropriate and effective cryptography in order to safeguard information security.
Communication security	Protecting information in networks and the corresponding information-processing systems.
Portability and interoperability	Providing the ability to securely operate the service on different IT platforms as well as the possibility of secure connections to different IT platforms and termination of the service.
Procurement, development and maintenance of information systems	Complying with the security targets in case of new developments and procurement of information systems as well as changes.

Section	Objective
Control and monitoring of service providers and suppliers	Protecting information that can be accessed by service providers and/or suppliers of the cloud provider (subcontractors) and monitoring the services and security requirements agreed upon.
Security incident management	Assuring a consistent and comprehensive approach regarding the monitoring, recording, assessment, communication and escalation of security incidents.
Business continuity management	Strategic establishment and governance of a business continuity management (BCM). Planning, implementing and testing business continuity concepts as well as incorporating safeguards in order to ensure and maintain continuous operations.
Security check and verification	Checking and verifying that the information security safeguards are implemented and carried out in accordance with the organisation-wide policies and instructions.
Compliance and data protection	Preventing violations against statutory or contractual duties with respect to information security.
Mobile device management	Guaranteeing secure access to IT systems via mobile devices in the cloud provider's responsibility to develop and operate the cloud service.

Table 1: Sections of C5 with assigned objectives

2.3 Underlying national and international standards

According to C5's objective, the content of the individual requirements were derived from nationally and internationally established standards. The following standards were taken into account:

» ISO/IEC 27001:2013

» CSA[3] – Cloud Controls Matrix 3.01 (CSA CCM)

» AICPA[4] – Trust Services Principles Criteria 2014 (TSP)

» ANSSI[5] Référentiel Secure Cloud v2.0 (version intermediaire validée du 20/03/2015, not published)

» IDW[6] ERS FAIT 5 (draft of a statement on accounting: "Grundsätze ordnungsmäßiger Buchführung bei Auslagerung von rechnungslegungsrelevanten Dienstleistungen einschließlich Cloud Computing" [Generally accepted accounting principles for the outsourcing of accounting-related services including cloud computing], version of 4 November 2014)

» BSI IT-Grundschutz Catalogues, 14th version 2014

» BSI SaaS Sicherheitsprofile 2014 (German only)

Providers who already hold the respective certifications or aligned their organisation and processes along one or several of these standards have the possibility to document the implementation of C5 largely through referencing their individual safeguards to the requirements of C5. In this respect, the user is supported by means of detailed references between the requirements of this catalogue and the requirements of the mentioned standards in a separate auxiliary document which can be found on the BSI websites.

[3] Cloud Security Alliance, a non-profit organisation for the distribution of security standards in the field of cloud computing

[4] American Institute of Certified Public Accountants

[5] Agence nationale de la sécurité des systèmes d'information, French authority for the security of information systems

[6] Institut der Wirtschaftsprüfer [Institute of Certified Public Accountants in Germany, Incorporated Association], serving the interests of the auditing professions in Germany

3 Proving conformity with the requirements by an independent audit

3 Proving conformity with the requirements by an independent audit

3.1 Introduction

The requirements in this document can be used by cloud providers and by cloud customers. The providers can use this as orientation for the secure design of their processes. The cloud customer will be entitled to demand verification of whether the cloud provider meets these requirements. An assessment for each individual customer would not be efficient for the provider and provides no sufficient reliability for the customer. Moreover, there would be no uniform level of information on security issues – if a customer sends inquiries to several providers – so that a customer could not compare different providers. According to the BSI's professional point of view, a uniform audit by an independent third party expert who creates a standardised report for the cloud provider to pass it on to customers and prospects is a cost-efficient and reasonable solution to this problem.

Below, the BSI presents its professional point of which auditors should follow when performing such an audit, irrespective of their individual responsibility, and how they have to report to the provider and the customer of the cloud service.

When designing the audit requirements, nationally and internationally established standards were taken into account in the same way as described before for the security requirements themselves.

Specifically, the international auditing standard ISAE[7] 3000 (Revised) is used as the general basis for the auditing and reporting. It is supplemented by additional auditing standards which – applied correspondingly – are to be used for specific questions regarding auditing and reporting. In this respect, ISAE 3402 or the auditing standard Prüfungsstandard (PS) 951 of the Institut der Wirtschaftsprüfer (IDW) are to be mentioned. Moreover, the rules for audits and documentation according to Service Operation Controls (SOC) must be respected.

Reference to targets and rules of national and international auditing and accounting is intentional. Furthermore, the special requirements for the independence of the auditor and the binding nature and comprehensibility of the audit evidence should be ensured. At the same time, cloud providers who have already been audited according to the standards mentioned in section 2.3 are thus able to re-use system descriptions already available and, where applicable, also parts of applicable audit results in parallel. These may serve as audit evidences within testation of the cloud service against C5. Thus, the additional audit effort can be reduced.

According to the BSI's professional point of view, the requirements for the audit in the mentioned auditing standards for the purposes of meaningful audit opinions must be fulfilled at all times. In the following section, several essential explanations are provided.

3.2 Auditing standards and criteria

3.2.1 ISAE 3000 (Revised) as auditing standard

Auditing and reporting shall be carried out by applying ISAE 3000 (Revised) "Assurance Engagements Other than Audits or Reviews of Historical Financial Information".

ISAE 3000 (Revised) describes general requirements for the qualification and conduct of an auditor (e. g. professional judgment and scepticism) as well as for accepting, planning and

[7] International Standard on Assurance Engagements

carrying out an audit engagement. Furthermore, the standard includes general requirements for audit criteria without specifying their content in more detail. ISAE 3000 (Revised) must therefore be understood as a high-level auditing standard which provides the required high-level framework.

The standard distinguishes between audits with reasonable assurance and audits with limited assurance. Furthermore, so-called “attestation engagements” are distinguished from so-called “direct engagements”.[8]

Audits regarding the implementation of the requirements of C5 presented here must be carried out with reasonable assurance as an “attestation engagement”. In case of an “attestation engagement”, the legal representatives of the cloud provider (e. g. a representative of the top management of the cloud provider) or the authorised signatories of the organisational unit responsible for the operations of the cloud service (hereinafter referred to as “management of the cloud provider”) issue a statement on the appropriateness and – where relevant – effectiveness of the safeguards established to meet the requirements. With this statement, the cloud provider signals his liability to implement the requirements to the cloud customer. For the auditor, the statement (which is internationally also referred to as “written assertion” or “written statement”) is the starting point for their audit.

3.2.2 Correspondingly applying further auditing standards

In case of special questions regarding the auditing procedure as well as documentation and reporting, ISAE 3402 “Assurance Reports on Controls at a Service Organization” is to be used correspondingly. As an alternative or supplement, the auditor can also refer to the German version of this standard (IDW PS 951 new version “Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen” [Auditing the internal control system of service companies]) and/or the US-American targets of the “Statements on Standards for Attestation Engagements” AT Section 801 and/or AT Section 101 for the use case of so-called SOC audits.

All these standards aim for appropriate and effective internal processes and controls which are used by the service provider in order to achieve specific targets and goals. For ISAE 3402, IDW PS 951 (new version) and AT Section 801, processes and controls have priority to the extent that they are important for the financial reporting of the service provider’s customers. In the special use case of SOC 2 audits according to AT Section 101, proof of the implementation of the AICPA Trust Services Principles and Criteria (security, availability, processing integrity, confidentiality and/or data protection) must be demonstrated. Moreover, these principles and criteria were also taken into consideration when drawing up C5 (see section 2.3).

Correspondingly applying these auditing standards means that the audit is based on the contents of the individual requirements of C5. The auditing standards mentioned here with regard to specific questions are used for audit planning, implementation and reporting. Accordingly, the requirements for the audit which are described in more detail in the sections 3.3 and 3.4 can be traced back directly to these auditing standards. Therefore, all interest groups involved (cloud provider, auditor and the customer as the addressee of the report) which already have experience with audits and/or reports according to these auditing standards can also use this experience directly for the audit along C5 and/or for evaluating the reporting.

For several aspects, however, the BSI has specific additional expectations. These expectations relate, for example, to the qualification of the auditor or details of the presentation of deviations identified in the reporting. They are summarised and explained in section 3.5 as “Separate and supplementary requirements of the BSI”.

[8] See ISAE 3000, marginal number 12.

3.2.3 Criteria

The audit criteria need to be based on the following high-level requirements (see correspondingly e. g. ISAE 3000 (Revised), marginal number A45 or IDW PS 951 new version, marginal number 50):

» **Relevance:** Criteria must be relevant for the assessment of the principles, procedures and safeguards established by the cloud provider as well as for the decision-making.

» **Completeness:** Criteria are complete if no aspects essential for the assessment of the principles, procedures and safeguards established by the cloud provider and no aspects essential for the decision-making were excluded.

» **Reliability:** Criteria are reliable if they allow for a consistent and comprehensible assessment of the principles, procedures and safeguards established by the cloud provider.

» **Neutrality:** Criteria are neutral if they ensure an objective assessment of the principles, procedures and safeguards established by the cloud provider.

» **Comprehensibility:** Criteria are comprehensible as far as they allow for clear conclusions and misinterpretations are thus avoided.

The requirements of C5 are based on the standards and publications listed in section 2.3. By means of this reference, it is ensured according to the BSI's point of view that the requirements included therein are suitable for use as a basis for a proper and comprehensible assessment of the cloud services by the cloud provider themselves and by an independent auditor.

3.3 Subject of the audit including system description

3.3.1 Subject of the audit

The subject of the audit includes the following two areas:

» Description of the internal control system related to the cloud services (system description) and

» Controls presented in the system description with reference to the individual requirements on the basis of a management statement of the cloud service provider

The responsibility for the system description and its content lies with the legal representatives of the provider. The management statement includes the appropriateness and usually also the effectiveness of the internal control system presented in the system description. The processes and procedures for implementing and executing the presented controls are also included.

For an audit regarding C5, a distinction is made between two types of audits and reporting, as is also the case in ISAE 3402 or IDW PS 951 new version.

» **Type 1 audit and reporting:** The auditor has to assess whether the system description properly reflects the actual design and implementation of the internal control system related to the cloud services at the time of the audit and whether the controls presented have been designed appropriately. For example, type 1 reporting is suitable, for initial audits of newly developed cloud services in order to obtain an audit result in a timely manner. It is not suitable for demonstrating effective implementation over a retrospective period of time.

» **Type 2 audit and reporting:** As compared to type 1 audit and reporting, the auditor performs additional audit activities with respect to the effectiveness of the controls (functional tests). For this purpose, the audit period usually covers twelve months, but not less than six months. Shorter audit periods can be taken into account in exceptional cases (e. g. foundation of the cloud provider, acquisition of new cloud services) and must be justified within the report.

According to the BSI's professional point of view, type 2 audit and reporting is required in order to provide an appropriate informative opinion. Type 1 reporting should only be carried out in the exceptional cases as mentioned above and must be justified and should under no circumstances be considered several times in a row.

C5 makes a distinction between basic requirements and additional requirements (see section 2.1).

- The audit and reporting can be based either on the basic requirements alone or on the basic requirements together with the additional requirements.

- The basic requirements (and, where applicable, the additional requirements) must be addressed completely and without omissions. To demonstrate a higher level of confidentiality, additional requirements relating to confidentiality can be taken into consideration (in section 5, column "C/A" classified with "C" and/or "C/A"). The same applies to demonstrating a higher level of availability. Which additional requirements were used as criteria for the audit must be reflected in the system description of the cloud provider. If all additional requirements relating to confidentiality (C and C/A) and/or all requirements with reference to availability (A and C/A) have been met in full, this must also be marked in the description of the subject of the audit by the supplement "The system description addresses all additional requirements regarding [the confidentiality]/[(and) the availability] in full". If individual requirements cannot be applied from the cloud provider's point of view, this is to be justified accordingly in the system description. The supplement in the description of the subject of the audit is omitted in this case.

3.3.2 System description of the cloud provider

The system description of the cloud services is created by the cloud provider. The minimum scope of the system description results from applying ISAE 3402 (or the standard(s) used as an alternative, see section 3.2) correspondingly. The following components have to be listed, for example:

- Type and scope of the provided cloud services

- Principles, procedures and measures for providing (development and/or operation) the cloud service, including the implemented controls

- Description of the infrastructure, network and system components used for the development and operation of the cloud service, including the geographical location of the data in use or at rest

- Regulation for handling significant incidents and conditions which constitute exceptions to regular operations, such as the failure of critical IT systems

- Roles and responsibilities of the cloud provider and the cloud customer, including the obligation to cooperate and required corresponding controls at the cloud customer

- Functions assigned or outsourced to subcontractors

For type 2 reporting, the system description must represent all essential changes to the internal control system related to the cloud services, which were made during the period covered, in a sufficiently detailed manner. This also includes those changes resulting from an update of C5 which has taken place in the meantime (see section 3.5.4).

Information which is relevant to the environment of the internal control system related to the cloud services must not be omitted or distorted in the system description. However, this does not include all aspects that can be considered to be important from the perspective of individual contractors or prospects.

In this respect, it must be noted that the system description is usually drawn up for a large number of cloud customers for whom the cloud provider may follow individual processes customized to meet individual cloud customer requirements.

In many cases, the cloud provider outsource parts of their business processes for the development and/or operation of the cloud service to other service companies (use of subcontractors). This must be taken into account accordingly in the system description (and also in the course of the audit). For this purpose, a distinction is made between the "inclusive method" and the "carve-out method".

- **Inclusive method:** The system description also includes the type and scope of the outsourced functions and the controls implemented at the subcontractor, which, together with the controls at the cloud provider themselves, are also subject of the audit.
- **Carve-out method:** The system description does not include a detailed description of the outsourced functions. The controls implemented at the subcontractor are not subject of the audit. In this case, at least the controls of the service provider which are used to monitor the effectiveness of the controls at the subcontractor are audited (see also the requirements DLL-01 and DLL-02 in section 5). The most straightforward approach in this case is if the subcontractor is audited (and will be audited regularly) according to the requirements of this document and submits an audit report on the effectiveness of the outsourced controls to the cloud provider, which the provider processes as part of their procedures used to control and monitor their subcontractors.

The cloud provider must select the method to be applied for his audit. This selection must be outlined clearly in the audit report and made transparent to the (potential) cloud customer. When the carve-out method is applied, the certified public auditor assesses whether the scope of the outsourcing is presented in the system description (e. g. on the basis of the contract and audit reports on the service-related internal control system of the subcontractor) and the effectiveness of the outsourced controls is monitored by the cloud provider according to requirement DLL-02.

To what extent subcontractors meet the requirements from this catalogue and how the surrounding parameters for transparency are designed at the subcontractor must be documented in the audit report.

3.3.3 Use of evidence from other audits

The requirements of C5 are largely based on nationally and internationally recognised standards. If those standards are already used by the cloud provider as references, the provider will have already aligned the processes and controls of his operations to the related requirements of C5. These processes and controls typically also constitute the basis for further audits which are carried out at the cloud provider, usually by independent external auditors. In this context, audits according to ISAE 3402, IDW PS 951 and/or the US- American regulations for SOC 1 or SOC 2 in particular should be mentioned.

In these cases, it is recommended to combine the organisation and timing of these audits with an audit according to C5. This enables the auditor and cloud provider, in case of overlapping controls, to use parts of the system descriptions and audit results for both the reporting according to ISAE 3402 and/or SOC 2, for example, and for the reporting according to C5. It usually makes sense to cover the same audit period for C5 as for the other audits.

This enables to reduce additional effort for covering the requirements of C5, for the documentation of the measures in a system description and for the audit itself.

If the cloud provider aims for further certificates (e. g. according to ISO/IEC 27001, ISO 22301 or data protection certificates), it is recommended to incorporate the corresponding auditors in the audit team and to perform a joint audit as far as practicable. This allows further optimisation of the audit efficiency. The reference table provided in a separate document for C5 may help to identify overlaps between the standards mentioned in section 2.3 and C5.

The auditor's other general possibilities of also using audit results as work of others are part of his or her individual responsibility and remain unaffected by the statements above.

3.4 Audit objective and reporting

3.4.1 Audit objective

With respect to the audit objective, a distinction has to be made as to whether type 1 or type 2 reporting (see section 3.3.1) has been agreed upon. Depending on the type, the auditor issues different audit opinions. The objective of the audit is to allow the auditor to issue a statement with reasonable assureance (audit opinion) as to whether

- the provider's system description properly reflects the actual design and implementation of the internal control system related to the cloud services at the point in time of the audit (type 1 reporting) and/or during the period of time to be audited (type 2 reporting),
- the controls presented in the system description at the time of the audit (type 1 reporting) and/or during the period of time to be audited (type 2 reporting) are designed appropriately with respect to the fulfilment of the requirements of C5 and
- the controls presented in the system description (only in the case of type 2 audit and reporting) were effective during the period of time to be audited.

3.4.2 Reporting of the auditor

The reporting on the audit includes the following elements (with corresponding application of ISAE 3402) and should be structured accordingly:

1. Independent auditor's report
   - Assignment and scope of the audit
   - Responsibility of the legal representatives of the cloud service provider and/or of the cloud provider management responsible for the cloud services
   - Independence and quality assurance of the auditor/auditing company, including information on the technical qualification of the auditor
   - Responsibility of the auditor
   - Inherent limits of controls at service companies
   - Audit opinion
   - Addressees and use of the certificate
   - Notes on the assignment conditions
2. Statement of the legal representatives of the cloud service provider and/or of the cloud provider management responsible for the cloud services (internationally also referred to as “written assertion” or “written statement”)
3. Description of the internal control system related to the cloud services (as part of the system description)
4. Presentation of the requirements and the assigned controls (part of the system description) as well as presentation of the audit activities carried out and the individual audit results of the auditor
5. Optionally: Other information, provided by the service provider

3.5 Separate and supplementary requirements of the BSI

3.5.1 Qualification of the auditor

According to the BSI's professional point of view, the assessment of an internal control system related to the cloud services on the basis of C5 puts special demands on the qualification of the auditor due to the technical nature of the associated requirements.

In addition to the general requirements for the auditor associated with the application of ISAE 3000 (Revised), the following supplementary requirements are imposed on the auditor respectively the audit team.

At least half of the members of the audit team has more than 3 years of professional experience in accounting (auditing) and, in addition to this, at least one of the following professional examinations/certifications:

- Information Systems Audit and Control Association (ISACA) – Certified Information Systems Auditor (CISA) or Certified Information Security Manager (CISM) or Certified in Risk and Information Systems Control (CRISC)

- ISO/IEC 27001 Lead Auditor or BSI-certified ISO 27001 Auditor for Audits on the basis of BSI IT-Grundschutz

- Cloud Security Alliance (CSA) – Certificate of Cloud Security Knowledge (CCSK)

- $(ISC)^2$ – Certified Cloud Security Professional (CCSP)

As part of the reporting, it must be specified which of the professional examinations/certifications are held by the audit team (e. g. in the section "Independence and quality assurance of the auditor"). Upon request, appropriate documents (e. g. certificates etc.) must be submitted to the client.

3.5.2 Reporting on existing and/or identified exceptions to the requirements

It is in the nature of audits that "negative" audit findings may come up during the course of an audit. Whether or not such a finding has an impact on the audit opinion, the customers of the cloud provider expect remediating measures for error correction as well as system and process optimisation to be performed.

For this reason, the following additional information must be included in the audit report:

- If the deficiency was identified by the service provider, it must be specified when and with which measures the deficiency was identified.

- If the deficiency had already been subject of the reporting over a previous audit period, it must be specified when and with which measures the deficiency was identified, in addition to a separate note that it was identified in a previous audit period. This assumes that the auditor has access to previous audit reports of the cloud provider. The auditor must seek separate assurance of this as part of his assignment.

- In any case, it should be specified which measures for the future elimination of the deficiency and the date when these measures will be completed and/or implemented effectively.

This can be reported, for example, in a separately marked section of the system description or in the optional section "Other information, provided by the service provider".

3.5.3 Information on the limitation of liability

Regulations regarding the auditor's liability to the service provider and other recipients of the report may be designed differently, also depending on country-specific regulations concerning the auditor.

In the BSI's professional point of view, specifications regarding the type and limit of the auditor's liability is important information for the recipient of the report and therefore must be included in the reporting according to the agreement.

Information on this can be provided, for example, in the section "Notes on the assignment conditions" (if necessary, with reference to further annexes).

3.5.4 Updates of C5

The BSI intends to update C5 regularly according to the general technical developments and to the continuous development of the underlying standards.

In this context, cloud providers and auditors shall have sufficient time to adjust systems and processes as well as the audit approach to updates of C5.

According to the BSI's professional point of view, the adjustments must be implemented within 12 months after the new version has been published. Any deviations from this must be justified towards customers and auditors.

As described in section 3.3.2, all relevant changes to the internal control system related to the cloud services which were made during the auditi period must be documented in the system description in a sufficiently detailed manner. Since updates of C5 must be implemented within 12 months, it may occur within an audit period that the assessment of the appropriateness and effectiveness relates to both the state before and after the implementation.

If the audit period ends between six and twelve months after the publication of the updated C5, the cloud provider must add specifications to the system description regarding the measures which are not yet implemented. This must also indicate when these measures are to be completed and/or implemented effectively.

3.6 Application notes for potential cloud customers: Regular audits and contractual assurance

The previous sections outline the basic requirements for audit and reporting of cloud services. The following chapters will describe the specific requirements of C5. In this section, the BSI provides potential cloud customers with hints on how to use available audit attestations of cloud providers.

First, it should be noted that the security of cloud services is an ongoing task. This understanding must also be reflected in the attestation which should therefore be renewed at regular intervals – usually every 12 months.

Moreover, the BSI does not have any influence on the actual audit by the certified public auditor and does not check the quality of the cloud service either. The certified public auditor performs their activities for the cloud provider and not for the customer of the provider.

The customer of the cloud provider should consider the compliance with the requirements of C5 (including the requirements for the audit, audit intervals and reporting) as an essential component of their assignment and contractually agree upon this with the provider. This applies particularly if additional requirements are to be met by the cloud provider.

Furthermore, the potential cloud customer should base their decision not only on an existing, current attestation (whether or not it relates solely to the basic requirements or also to additional requirements) according to C5, but should also request the audit report at regular intervals.

4 Framework conditions of the cloud service (surrounding parameters for transparency)

4 Framework conditions of the cloud service (surrounding parameters for transparency)

Objective: The general organisational and legal framework conditions and targets are described comprehensibly and accurately for a third party expert in order to assess the general suitability of the cloud service for the desired application.

UP-01 System description

Basic requirement

In their system description, the cloud provider provides comprehensible and transparent specifications regarding the cloud service, which allow an expert third party to assess the general suitability of the cloud service for the desired application. The system description describes the following aspects:

- Type and scope of the cloud services rendered according to the service level agreement which is typically based on a contract concluded with the cloud customers
- Principles, procedures and safeguards for rendering (development and/or operation) the cloud service, including the controls established
- Description of the infrastructure, network and system components used for the development and operation of the cloud service
- Handling of significant incidents and conditions which constitute exceptions to regular operations, such as the failure of critical IT systems
- Roles and responsibilities of the cloud provider and the cloud customer, including the duties to cooperate and corresponding controls at the cloud customer
- Functions assigned or outsourced to subcontractors

Supplementary information for the basic requirement

The description of the infrastructure, network and system components should be sufficiently detailed so that the cloud customer gains a good overview that is necessary for risk assessment as part of their security management, but without putting the security of the cloud provider at risk by this documentation.

UP-02 Jurisdiction and data storage, processing and backup locations

Basic requirement

In service level agreements, their process documentation or comparable documentation, the cloud provider provides comprehensible and transparent specifications regarding its jurisdiction as well as with respect to data storage, processing and backup locations, which allow an expert third party to assess the general suitability of the cloud service for the customer application. This also holds true if data of the cloud customer is processed, stored and backed up by subcontractors of the cloud provider. Data of the cloud customer shall only be processed, stored and backed up outside the contractually agreed locations only with the prior express written consent of the cloud customer.

UP-03 Disclosure and investigatory powers

Basic requirement

In service level agreements, their process documentation or comparable documentation, the cloud provider provides comprehensible and transparent specifications regarding applicable disclosure and investigatory powers of government agencies which allow access to data of the cloud customer. The specifications must allow an expert third party to assess the general suitability of the cloud service for the customer application. If the cloud provider accesses third-party services, the provider has obtained these specifications from them.

Supplementary information for the basic requirement

Affiliated companies are parent or subsidiary companies of the cloud provider within the meaning of § 271 Para. 2 HGB [German Commercial Code]. Disclosure and investigatory powers usually exist towards the police and the public prosecutor's office as well as intelligence agencies.

UP-04 Certifications

Basic requirement

In service level agreements, their process documentation or comparable documentation, the cloud provider provides comprehensible and transparent specifications regarding available and valid certifications and certificates of independent third parties, which allow an expert third party to assess the general suitability of the cloud service for the customer application.

Supplementary information for the basic requirement

The following certifications or certificates may be submitted:

- ISO/IEC 27001 (if necessary, also based on IT-Grundschutz)
- ISO 22301
- Proof of compliance with data protection accepted by the responsible data protection authorities
- Audit reports according to ISAE 3402/SSAE 16/ SOC 1/IDW PS 951
- Software certificates according to IDW PS 880

In this respect, the target of certification and/ or, in the case of system certifications, the corresponding scope is important.

5 Objectives and requirements

5 Objectives and requirements

5.1 Organisation of information security

Objective: Planning, implementation, maintenance and continuous improvement of a framework regarding information security within the organisation.

OIS-01 Information security management system (ISMS)

Basic requirement

The top management initiates, controls and monitors an information security management system (ISMS) which is based on ISO standards of the 2700x series.

- The instruments and methods used allow a comprehensible control of the following tasks and activities to permanently maintain and ensure information security: Planning, implementing the plan and/or carrying out the project
- Performance review and/or monitoring the achievement of objectives
- Eliminating discovered flaws and weaknesses and continuous improvement.

The ISMS also includes the IT processes for the development and operation of the cloud service.

Supplementary information for the basic requirement

If the cloud provider cannot submit a certification of the ISMS yet, the statement of applicability of which covers the IT processes for the development and operation of the cloud service, appropriateness and effectiveness can be assessed, among other things, by auditing the following requirements:

- Strategic targets regarding information security and responsibility of the top management (OIS-02)
- Identification, analysis, assessment and handling of risks (OIS-07)
- Policies and instructions (SA-01, SA-02 and SA-03)
- Notification of the top management (SPN-01)

Description of additional requirements (confidentiality and availability)

The top management initiates, controls and monitors an information security management system (ISMS), which has a valid certification according to ISO/IEC 27001:2013 or ISO 27001 on the basis of IT- Grundschutz. The statement of applicability covers the IT processes for the development and operation of the cloud service.

OIS-02 Strategic targets regarding information security and responsibility of the top management

Basic requirement

A security policy with security objectives and strategic parameters for achieving these objectives is documented. The security objectives are derived from the corporate objectives and business processes, relevant laws and regulations as well as the current and future expected threat environment with respect to information security. The strategic targets constitute essential framework conditions which in further policies and instructions are specified in more detail (see SA- 01). The security policy is adopted by the top management and communicated to all concerned internal and external parties of the cloud provider (e.g. cloud customers, subcontractors).

Supplementary information for the basic requirement

The security policy required here is a basic requirement. Further policies and instructions must be based on the size and complexity of the organisation of the cloud provider and the type of the cloud service offered.
Whereas the general security objectives and a strategy to achieve these objectives have to be formulated concisely in the security policy, it typically does not include organisational and technical details. It has proved to be successful to regulate these details in further policies and instructions on different levels. At the lower levels, the level of detail increases, while the change intervals are reduced.

OIS-03 Authorities and responsibilities in the framework of information security

Basic requirement

Responsibilities shared between the cloud provider and cloud customers, duties to cooperate as well as interfaces for the reporting of security incidents and malfunctions are defined, documented, assigned depending on the respective cloud model (infrastructure, platform or software as a service) and the contractual duties and communicated to all concerned internal and external parties (e. g. cloud customers, subcontractors of the cloud provider). On the part of the cloud provider, at least the following roles (or comparable equivalents) are described in the security policy or associated policies and corresponding responsibilities assigned:

» Head of IT (CIO)

» IT Security Officer (CISO)

» Representative for the handling of IT security incidents (e. g. Head of CERT)

Changes to the responsibilities and interfaces are communicated internally and externally in such a timely manner that all internal and external parties concerned (e. g. cloud customers) are able to respond to them appropriately with organisational and technical safeguards, before the change becomes effective.

Supplementary information for the basic requirement

Documentation and job profiles which define and determine the authorities in the framework of information security should be available.
The appropriateness of the assignment of roles and responsibilities to one or several persons at the cloud provider must be assessed against the backdrop of the size and complexity of the organisation.

Description of additional requirements (confidentiality)

The cloud provider identifies all risks related to overlapping or incompatible authorities and responsibilities.

OIS-04 Separation of functions

Basic requirement

Organisational and technical controls are established in order to ensure the separation of roles and responsibilities (also referred to the “separation of duties”) which are incompatible with respect to the confidentiality, integrity and availability of information of the cloud customers. Controls for the separation of functions are established in the following areas in particular:

» Administration of roles, granting and assignment of access authorisations for users under the responsibility of the cloud provider

» Development and implementation of changes to the cloud service

» Maintenance of the physical and logical IT infrastructure relevant to the cloud service (networks, operating systems, databases) and the IT applications if they are in the cloud provider’s area of responsibility according to the contractual agreements with the cloud customers

Operative and controlling functions should not be performed by one and the same person at the same time. If it is not possible to achieve a separation of duties for organisational or technical reasons, appropriate compensating controls are established in order to prevent or uncover improper activities.

Description of additional requirements (confidentiality)

The cloud provider has documented any function separation conflicts and the compensating controls established for this purpose comprehensibly (e. g. in a role and rights concept) to allow for an assessment of the appropriateness and effectiveness of these controls.

OIS-05 Contact with relevant government agencies and interest groups

Basic requirement

Appropriate and relevant contacts of the cloud provider with government agencies and interest groups are established to be always informed about current threat scenarios and countermeasures.

Supplementary information for the basic requirements

Relevant contacts include, for example:

» Federal Office for Information Security (BSI) (or comparable agencies in other countries)

» OWASP Foundation

» CERT alliances DFN-CERT, TF-CSIRT etc.

Description of additional requirements (confidentiality and availability)

Procedures are defined and documented to communicate the information received to the internal and external employees of the cloud provider and to be able to respond to it appropriately and in a timely manner.

OIS-06 Policy for the organization of the risk management

Basic requirement

Policies and instructions for the general procedure applicable to the identification, analysis, assessment and handling of risks and IT risks in particular are documented, communicated and provided according to SA-01.

OIS-07 Identification, analysis, assessment and handling of risks

Basic requirement

The procedures for the identification, analysis, assessment and handling of risks, including the IT risks relevant to the cloud service are done at least once a year in order to take internal and external changes and influencing factors into account. The identified risks are comprehensibly documented, assessed and provided with mitigating safeguards according to the safeguards of the risk management.

Supplementary information for the basic requirement

If the cloud provider is a German Aktiengesellschaft (AG) [public limited company] or a German Kommanditgesellschaft auf Aktien (KGaA) [partnership limited to shares], § 91 Para. 2 AktG [German Public Companies Act] is applied. According to this, the board of directors must take suitable safeguards, i.e. especially establish a monitoring system so that developments putting the company at risk are detected at an early stage. If these safeguards have already been the subject of an audit carried out by a certified public auditor, these results can be taken into account. In this respect, it must be ensured that the risks relevant to the cloud service (usually IT risks) are the subject of the monitoring system audited. If business processes for the development and/or operation of the cloud service are outsourced to other service companies, the cloud provider still remains responsible for these risks. They must be addressed by appropriate procedures for the selection, control and monitoring of the service companies (see requirements DLL-01 and DLL-02).

Description of additional requirements (confidentiality and availability)

Parameters of the top management for the risk appetite and the risk tolerances of the cloud provider are included in the policy for the risk management or a comparable official document. The timely implementation of the mitigating safeguards is monitored by qualified personnel of the cloud provider. The top management is informed of the status of the identified risks and mitigating safeguards at least once every three months and in an appropriate form.

5.2 Security policies and work instructions

Objective: Providing policies and instructions with respect to the security claim and to support the business requirements.

■ SA-01 Documentation, communication and provision of policies and instructions

Basic requirement

Policies and instructions for information security or related topics derived from the security policy are documented in an uniform structure. They are communicated and made available to all internal and external employees of the cloud provider properly and adequately. Policies are versioned and approved by top management of the cloud provider. The policies and instructions describe at least the following aspects:

- Goals
- Scopes of application
- Roles and responsibilities, including requirements for the qualification of the personnel and the establishment of substitution arrangements
- Coordination of different company departments
- Security architecture and safeguards for the protection of data, IT applications and IT infrastructures which are managed by the cloud provider or third parties
- Safeguards for the compliance with legal and regulatory requirements (compliance)

Supplementary information for the basic requirement

Proper and adequate communication and provision must be assessed with respect to the size and complexity of the cloud provider's organisation and the type of the cloud service offered. Possible criteria include:

- Addressing the topic of policies and instructions when new employees start their work

- Training and information campaigns when approving new or revising existing policies and instructions

- Form of provision

Policies and instructions are required for the following basic requirements and specified in more detail in the corresponding controls (see brackets below):

- Risk management (OIS-06)

- Management of data media (AM-07)

- Maintenance of infrastructure and devices (PS-05)

- Data backup and restore (RB-06)

- Logging and monitoring (RB-10/RB-11)

- Identification and handling of vulnerabilities (RB-19)

- Management of system and data access authorisations (IDM-01)

- Cryptography and key management (KRY-01)

- Communication security (KOS-05)

- Portability and interoperability (PI-03)

- Procurement and development of cloud services (BEI-01)

- Change management (BEI-03)

- Policies for the handling of and security requirements for service providers and suppliers of the cloud provider (DLL-01)

- Business continuity management (BCM-02)

- Security of mobile terminal devices (MDM-01)

SA-02 Review and approval of policies and instructions

Basic requirement

The policies and instructions for information security are reviewed with respect to their appropriateness and effectiveness by specialists of the cloud provider who are familiar with the topic at least once a year. At least the following aspects are taken into account in the review:

- Organisational changes at the cloud provider

- Current and future expected threat environment regarding information security

- Legal and technical changes in the cloud provider’s environment

Revised policies and instructions are approved by committees or bodies of the cloud provider authorised to do so before they become valid.

Description of additional requirements (confidentiality and availability)

The regular review is followed up by central bodies at the cloud provider.

SA-03 Deviations from existing policies and instructions

Basic requirement

Exceptions of policies and instructions for information security are approved by committees or bodies of the cloud provider authorised to do so in a documented form. The appropriateness of approved exceptions and the assessment of the risks resulting from this are reviewed by specialists of the cloud provider who are familiar with the topic against the backdrop of the current and future expected threat environment regarding information security at least once a year.

Description of additional requirements (confidentiality and availability)

The appropriateness of approved exceptions and the assessment of the risks resulting from this are reviewed by an independent third party at least once a year as to whether they reflect a realistic picture of the current and future expected threat environment regarding information security (see SPN-01).

5.3 Personnel

Objective: Making sure that employees, service providers and suppliers understand their tasks, that they are aware of their responsibility with regard to information security and that the assets of the organisation are protected if the tasks are modified or completed.

HR-01 Security check of the background information

Basic requirement

The background of all internal and external employees of the cloud provider with access to data of the cloud customers or of the shared IT infrastructure is checked according to the local legislation and regulation by the cloud provider prior to the start of the employment relationship. To the extent permitted by law, the security check includes the following areas:

» Verification of the person by means of the identity card

» Verification of the curriculum vitae

» Verification of academic titles and degrees

» Request of a police clearance certificate for sensitive posts in the company

Supplementary information for the basic requirement

The security check can be supported by a specialised service provider. If employees of a service provider have access to the user data, the service provider must meet this requirement and make it transparent according to DLL-01 and DLL-02.

Description of additional requirements (confidentiality)

Special approval procedure in the hiring process for employees and posts for which particularly sensitive information is accessed are established.

HR-02 Employment agreements

Basic requirement

Employment agreements include the obligations of the cloud provider's internal and external employees to comply with relevant laws, regulations and provisions regarding information security (see KOS-10). The security policy as well as the policies and instructions for information security derived from this are added to the employment agreement documents. Corresponding compliance is confirmed by the employee by a written statement before they can access the data of the cloud customers or the (shared) IT infrastructure.

HR-03 Security training and awareness-raising programme

Basic requirement

A security training and awareness-raising programme tailored to specific target groups on the topic of information security is available and mandatory for all internal and external employees of the cloud provider. The programme is updated at regular intervals with respect to the applicable policies and instructions, the assigned roles and responsibilities as well as the known threats and must then be run through again. The programme includes at least the following contents:

» Regular and documented instruction on the secure configuration and secure operation of the IT applications and IT infrastructure required for the cloud service, including mobile terminal devices

» Appropriate handling of data of the cloud customers

» Regular and documented instruction on known basic threats and

» Regular and documented training on the behaviour in case of security-relevant events.

External service providers and suppliers of the cloud provider, who contribute to the development or operation of the cloud service, are obliged by contract to make their employees and subcontractors aware of the specific security requirements of the cloud provider and train their employees generally in the subject of information security.

Description of additional requirements (confidentiality and availability)

The programme takes different profiles into account and includes further information for posts and employees who have extensive authorisations or access to sensitive data. External employees of service providers and suppliers of the cloud provider, who contribute to the development or operation of the cloud service, are instructed in the specific security requirements of the cloud provider as well as generally in the subject of information security. The cloud provider checks on a random basis that the service providers and suppliers have carried out the instruction in an appropriate manner. The results of the audit are documented comprehensibly.

HR-04 Disciplinary measures

Basic requirement

A process for performing disciplinary measures is implemented and communicated to the employees in order to make the consequences of violations of the applicable policies and instructions as well as legal provisions and laws transparent.

HR-05 Termination of the employment relationship or changes to the responsibilities

Basic requirement

Internal as well as external employees are informed that the obligations to comply with relevant laws, regulations and provisions regarding information security remain valid even if the area of responsibility changes or the employment relationship is terminated.

5.4 Asset management

Objective: Identifying the organisation's own assets and the persons responsible and ensuring an appropriate level of protection.

AM-01 Asset inventory

Basic requirement

The assets (e. g. PCs, peripheral devices, telephones, network components, servers, installation documentation, process instructions, IT applications, tools) used to render the cloud service are identified and inventoried. By means of appropriate processes and safeguards, it is ensured that this inventory remains complete, correct, up-to-date and consistent. A history of the changes to the entries in the inventory is kept in a comprehensible manner. If no effective automatic procedures are established for this, this is ensured by a manual review of the inventory data of the assets which takes place at least once a month.

Supplementary information for the basic requirement

For asset management, see also ISO standards 55001 and 55002.

Description of additional requirements (availability)

In the event of a failure of assets which are of essential importance for the availability of the cloud service (e. g. central network components), the cloud provider is able to promptly detect which cloud customers are affected by this in order to ensure a response to the malfunctions occurred that complies with the service level agreement. By means of technical safeguards, it is ensured that the inventory of the assets is updated automatically at regular intervals.

AM-02 Assignment of persons responsible for assets

Basic requirement

All inventoried assets are assigned to a person responsible on the part of the cloud provider. The persons responsible of the cloud provider are responsible over the entire life cycle of the assets to ensure that they are inventoried completely and classified correctly.

AM-03 Instruction manuals for assets

Basic requirement

Policies and instructions with technical and organisational safeguards for the proper handling of assets are documented, communicated and provided according to SA-01 in the respectively current version.

AM-04 Handing in and returning assets

Basic requirement

All internal and external employees of the cloud provider are obliged to return or irrevocably delete all assets which were handed over to them in relation to the cloud service and/or for which they are responsible as soon as the employment relationship has been terminated.

AM-05 Classification of information

Basic requirement

The cloud provider uses a uniform classification of information and assets which are relevant to the development and rendering of the cloud service.

Supplementary information for the basic requirement

The classification of information and assets should, among other things, take the following specifications into consideration:

- Criticality for the rendering of the cloud service
- Sensitivity to unauthorised disclosure or modification
- Data type
- Applicable legislation of the assets
- Geographical location
- Context
- Legal restrictions
- Contractual restrictions
- Value

AM-06 Labelling of information and handling of assets

Basic requirement

Work instructions and processes for the implemented classification scheme of information and assets are in place in order to ensure the labeling of information as well as the corresponding handling of assets. This only refers to assets which store or process information.

Supplementary information for the basic requirement

The labeling of information must be carried out after the classification has been performed and is usually the responsibility of the asset owners. A labeling method could be a provision for documents so that the confidentiality level is specified in the same place on each page of the document. Methods for the handling of assets should include information as to how assets are to be protected according to each confidentiality level.

AM-07 Management of data media

Basic requirement

Policies and instructions with technical and organisational safeguards for the secure handling of data media of any type are documented, communicated and provided according to SA-01. The targets establish a reference to the classification of information (see AM-05). They include the secure use, the secure transport as well as the irrevocable deletion and destruction of data media.

Supplementary information for the basic requirement

Policies and instructions should take the following aspects into account:

- Secure and irrevocable deletion of the data and disposal/destruction of the data media
- Encryption of removable media
- Transmission of data to new data media when a medium is replaced

AM-08 Transfer and removal of assets

Basic requirement

Devices, hardware, software or data may only be transferred to external premises after it has been approved by authorised committees or bodies of the cloud provider. The transfer takes place securely according to the type of the assets to be transferred.

5.5 Physical security

Objective: Preventing unauthorised physical site access and protection against theft, damage, loss and failure of operations.

PS-01 Perimeter protection

Basic requirement

The perimeter of premises or buildings which house sensitive or critical information, information systems or other network infrastructure are protected in a physically solid manner and by means of appropriate security safeguards that conform to the current state of the art.

Supplementary information for the basic requirement

Possible security safeguards could include, for example, fences, walls, security guards or video monitoring. For the outer doors and windows, burglar-resistant material (e.g. according to DIN EN 1627 resistance class RC 2) and corresponding closing devices should be installed.

Description of additional requirements (confidentiality)

The security concept includes the setup of different security zones which are separated by security lines as monitored and secured gateways between the zones.

PS-02 Physical site access control

Basic requirement

Access to the premises or buildings which house sensitive or critical information, information systems or other network infrastructure is secured and monitored by means of physical site access controls in order to avoid unauthorised site access.

Description of additional requirements (confidentiality)

The physical site access controls require two-factor authentication.

PS-03 Protection against threats from outside and from the environment

Basic requirement

Structural, technical and organisational safeguards are taken to protect premises or buildings which house sensitive or critical information, information systems or other network infrastructure against fire, water, earthquakes, explosions, civil disturbances and other forms of natural threats and threats caused by humans. At two geo-redundant sites, at least the following safeguards are carried out:

Structural safeguards:

- » Setup of a separate fire zone for the computer centre
- » Use of fire-resistant materials according to DIN 4102-1 or EN 13501 (period of fire resistance of at least 90 minutes)

Technical safeguards:

- » Sensors to monitor temperature and humidity
- » Connecting the building to a fire alarm system with notification of the local fire department
- » Early fire detection and extinguishing systems

Organisational safeguards:

- » Regular fire drills and fire safety inspections to check compliance with fire protection measures

Description of additional requirements (availability)

The environmental parameters are monitored. If the tolerable control range is exceeded from below or above, alarm messages are generated and forwarded to the responsible bodies.

PS-04 Protection against interruptions caused by power failures and other such risks

Basic requirement

Precautions against the failure of supply services such as power, cooling or network connections are taken by means of suitable safeguards and redundancies in coordination with safeguards for operational reliability. Power and telecommunication supply lines which transport data or supply information systems must be protected against interception and damage.

Supplementary information for the basic requirement

Suitable safeguards for precautions typically include the following:

- Redundant power supply and air conditioning systems
- Use of appropriately dimensioned uninterruptible power supplies (UPS) and emergency power systems (EPS)
- Redundant network connection via different physical connections

Furthermore, the cloud provider should determine and communicate which external temperatures the air conditioning of the computer centre can withstand for how long (e. g. 30°C/14 days, 35°C/6 days, 40°C/4 days). If river water is used for cooling, it should be specified at which water levels the air conditioning can be maintained for how long. To demonstrate resilience against interception and the protection against damage, wiring diagrams and a corresponding protection concept can be submitted, which is checked for plausibility in discussion with the person responsible. During visual inspection, attention should be paid, among other things, to traces of violent opening attempts at closed distributors, currency of the documentation inside the distributors, conformity of the actual wiring and patches with the documentation, intactness of the short circuits and grounding of non-required lines as well as for impermissible installations and changes.

Description of additional requirements (availability)

The supply services are monitored. If the tolerable control range is exceeded from below or above, alarm messages are generated and forwarded to the responsible bodies. The cloud provider determines and communicates the times of self-sufficient supply which are achieved by the safeguards taken if the supply services fail or if extraordinary events occur (e. g. heat waves, long lasting power failure) as well as the maximum tolerable times for a failure of the supply services. Contracts for maintaining the precautions with corresponding service providers have been concluded (e. g. for the fuel of the emergency power supply).

PS-05 Maintenance of infrastructure and devices

Basic requirement

Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 which describe the maintenance (especially remote maintenance), deletion, updating and re-use of assets in information processing in outsourced premises or by external personnel.

Supplementary information for the basic requirement

Policies and instructions should take the following aspects into account:

- Secure deletion of sensitive data prior to external repair or maintenance
- Analyses of the assets prior to re-use in order to avoid manipulations or malfunctions
- Renewal of assets if availability, security, integrity or confidentiality could be at risk

5.6 Operations

Objective: Ensuring proper regular operations including appropriate safeguards for planning and monitoring the capacity, protection against malware, logging and monitoring events as well as handling vulnerabilities, malfunctions and errors.

RB-01 Capacity management – planning

Basic requirement

The planning of capacities and resources (personnel and IT resources) follows an established procedure in order to avoid capacity bottlenecks. The procedures include forecasts of future capacity requirements in order to identify use trends and master system overload risks.

Supplementary information for the basic requirement

For economic reasons, cloud providers typically strive for a high utilisation of the IT resources (CPU, memory, storage space, network). In multi-client environments, the available resources must still be distributed between the cloud users (clients) so that the service level agreements are complied with. In this respect, the appropriate planning and monitoring of IT resources is critical to the availability and competitiveness of the cloud service. If the procedures are not documented or are subject to a higher confidentiality level as a trade secret of the cloud provider, it must be possible to explain the procedures as part of this audit at least orally.

Description of additional requirements (availability)

The forecasts are taken into account in coordination with the service level agreement for the planning and preparation of the provisioning.

RB-02 Capacity management – monitoring

Basic requirement

Technical and organisational safeguards for the monitoring and provisioning and de-provisioning of cloud services are defined. Thus, the cloud provider ensures that resources are provided and/or services are rendered according to the contractual agreements and that compliance with the service level agreements is ensured.

Supplementary information for the basic requirement

Technical and organisational safeguards typically include the following:

» Use of monitoring tools with alarm function if Defined thresholds are exceeded

» Process for correlating events and interface with incident management

» Continuous monitoring of the systems by qualified personnel

» Redundancies in the IT systems

Description of additional requirements (availability)

To monitor the capacity and the availability, the cloud customer is provided with relevant information via a self-service portal.

RB-03 Capacity management – data location

Basic requirement

The cloud customer is able to determine the locations (city/country) of the data processing and storage including data backups.

Supplementary information for the basic requirement

This requirement supplements requirement UP-02 in which the locations are to be documented. If a cloud provider renders their services at several sites, this requirement demands the cloud provider to define precisely at which site the service is rendered and the data processed.

RB-04 Capacity management – control of resources

Basic requirement

In case of IaaS/PaaS, the cloud customer is able to control and monitor the distribution of the system resources assigned to them for administration/use (e. g. computing capacity or storage capacity) in order to prevent resources from being congested.

RB-05 Protection against malware

Basic requirement

The logical and physical IT systems which the cloud provider uses for the development and rendering of the cloud service as well as the network perimeters which are subject to the cloud provider's area of responsibility are equipped with anti-virus protection and repair programs which allow for a signature- and behaviour-based detection and removal of malware. The programs are updated according to the contractual agreements concluded with the manufacturer(s), but at least once a day.

Description of additional requirements (confidentiality and availability)

The cloud provider draws up regular reports on the performed audits, which are reviewed and analysed by authorised bodies or committees. Policies and instructions describe the technical safeguards for the secure configuration and monitoring of the management console (both the self- service of the customer and the cloud administration of the service provider) in order to protect them against malware. The update is performed with the highest frequency that is contractually offered by the manufacturer(s).

RB-06 Data backup and restoration – concept

Basic requirement

Policies and instructions with technical and organisational safeguards in order to avoid losing data are documented, communicated and provided according to SA-01. They provide reliable procedures for the regular backup (backup as well as snapshots, where applicable) and restoration of data. The scope, frequency and duration of the retention comply with the contractual agreements concluded with the cloud customers as well as the cloud provider's business requirements. Access to the data backed up is limited to authorised personnel. Restoration procedures include control mechanisms that ensure that restorations are carried out only after they have been approved by persons authorised to do so according to the contractual agreements with the cloud customers or the internal policies of the cloud provider.

Supplementary information for the basic requirement

When making data backups, a distinction must be made between backups and snapshots of virtual machines. Snapshots do not replace backups, but can be part of the backup strategy in order to achieve the recovery point objectives (RPO) provided that they are stored additionally outside the original data location. The business requirements of the cloud provider for the scope, frequency and duration of the data backup are derived from the business impact analysis (see control BCM-03) for development and operating processes of the cloud service. If there are different data backup and restoration procedures for data under the responsibility of the cloud customer and the cloud provider, both versions are to be involved in an audit according to C5. For procedures applied to the backup of the cloud provider's data, only evidence of the appropriateness and implementation of the controls must be demonstrated, but not of their effectiveness. For procedures applied to the backup of the cloud customers' data, evidence of their effectiveness must also be demonstrated.

Description of additional requirements (confidentiality)

The data is backed up in encrypted form that conforms to the current state of the art.

RB-07 Data backup and restoration – monitoring

Basic requirement

The process of backing up data is monitored by means of technical and organisational safeguards. Malfunctions are examined and eliminated promptly by qualified employees in order to ensure compliance with the contractual duties towards the cloud customers or the cloud provider's business requirements with respect to the scope, frequency and duration of the retention.

Description of additional requirements (availability)

To monitor the data backup, the cloud customer is provided with the relevant logs or the summary of the results via a self-service portal.

RB-08 Data backup and restoration – regular tests

Basic requirement

Backup media and restoration procedures must be tested with dedicated test media by qualified employees at regular intervals. The tests are designed in such a way that the reliability of the backup media and the restoration time can be audited with sufficient certainty. The tests are carried out by qualified employees and the results documented comprehensibly. Any occurring errors are eliminated in a timely manner.

Description of additional requirements (availability)

Upon customer request, the cloud provider informs the cloud customers of the results of the restoration tests. Restoration tests are incorporated into the business continuity management of the cloud provider.

RB-09 Data backup and restoration – storage

Basic requirement

The data to be backed up is transmitted to a remote site (e. g. another data centre of the cloud provider) or transported to a remote site on backup media. If the backup of the data is transmitted to the remote site via a network, this is carried out in an encrypted form that conforms to the state of the art. The distance to the main site should be large enough to ensure that catastrophes there do not lead to a loss of data at the remote site and, at the same time, short enough to be able to fulfill the contractual duties regarding the restoration times. The safeguards taken to ensure the physical and environment-related security at the remote site corresponds to the level at the main site.

RB-10 Logging and monitoring – concept

Basic requirement

Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 in order to log events on all assets which are used for the development or operation of the cloud service and to store them in a central place. The logging includes defined events which may impair the security and availability of the cloud service, including logging the activation, stopping and pausing of different logs. In case of unexpected or unusual events, the logs are checked by authorised personnel due to special events in order to allow for a timely examination of malfunctions and security incidents as well as for the initiation of suitable safeguards.

Supplementary information for the basic requirement

Security-relevant events include, among other things:

» Login and logout processes

» Creation, change or deletion of users and extension of authorisations

» Use, extension and changes of privileged data access authorisations

» Use of temporary authorisations

Since the logged data is usually personal data, the data protection-related requirements for retention must be taken into account and checked in this case. Experience has shown that a retention period of one year should not be exceeded.

RB-11 Logging and monitoring – meta data

Basic requirement

Policies and instructions with technical and organisational safeguards for the secure handling of meta data (user data) are documented, communicated and provided according to SA-01. The meta data is collected and used only for accounting and billing purposes, for eliminating malfunctions and errors (incident management) as well as for processing security incidents (security incident management). The meta data is not used for commercial purposes. Meta data must be deleted immediately once it is no longer required to fulfill the legitimate purpose according to this requirement. The period of time during which meta data is retained is determined by the cloud provider. It is reasonably related to the purposes pursued with the collection of meta data.

Supplementary information for the basic requirement

Meta data is all data which arises at the cloud provider when their service is used by the cloud customer and which is not content data. This includes, among other things, login/logout times, IP addresses, GPS position of the customer, which resources (network, storage, computer) were used, which data was accessed when, with whom the data was shared, who was communicated with etc. Part of this data is used for accounting and billing purposes and for the (security) incident management. Moreover, it is also suitable for making the customer behaviour and (depending on the cloud service) a large part of decision-making and work processes transparent for the cloud provider. With the requirement, the collection and use of the meta data should be limited in a transparent and clear manner.

RB-12 Logging and monitoring – critical assets

Basic requirement

The cloud provider maintains a list of all assets critical in terms of logging and monitoring and reviews this list for their currency and correctness at regular intervals. For these critical assets, advanced logging and monitoring safeguards were defined.

RB-13 Logging and monitoring – storage of the logs

Basic requirement

The generated logs are stored on central logging servers on which they are protected against unauthorised access and changes. Logged data must be deleted immediately once they are no longer required to fulfill the purpose. Authentication takes place between the logging servers and the logged assets in order to protect the integrity and authenticity of the transmitted and stored information. The transmission is encrypted that conforms to the state of the art or via a separate administration network (out-of-band management).

Description of additional requirements (confidentiality)

Upon request of the cloud customer, the cloud provider offers customer- specific logging (in terms of the scope and duration of the storage) and makes it available to the customer. Depending on the protection requirements and technical feasibility, the logged data and the user data should be separated logically or physically.

RB-14 Logging and monitoring – accountability

Basic requirement

The generated logs allow for a clear identification of user access to the tenant level in order to support (forensic) analyses in the case of a security incident.

Supplementary information for the basic requirement

The logs should contain the following information:

» User ID

» Date and time

» Source & target (e. g. identity or name of the affected data, system components or resources)

» Activities carried out

» Information about success or failure of the access

Description of additional requirements (confidentiality)

Upon request of the cloud customer, the cloud provider makes the logs affecting them available promptly and in an appropriate form so that they can examine the incidents affecting them themselves.

RB-15 Logging and monitoring – configuration

Basic requirement

The access and management of the logging and monitoring functionalities is limited to selected and authorised employees of the cloud provider. Changes to the logging and monitoring are checked by independent and authorised employees and approved beforehand.

Description of additional requirements (confidentiality)

The access and management of the logging and monitoring functionalities requires multi-factor authentication.

RB-16 Logging and monitoring – availability of the monitoring software

Basic requirement

The availability of the logging and monitoring software is monitored independently. In case the logging and monitoring software fails, the responsible employees are informed immediately.

Description of additional requirements (confidentiality and availability)

The logging and monitoring software is designed redundantly in order to also monitor the security and availability of the customer systems in the event of failures.

RB-17 Handling of vulnerabilities, malfunctions and errors – concept

Basic requirement

Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 in order to ensure the prompt identification and addressing of vulnerabilities over all levels of the cloud service, for which they are responsible. The safeguards include among other things:

- Regular identification and analysis of vulnerabilities
- Regular follow-up of safeguards in order to address identified safeguards (e. g. installation of security updates according to internal target specifications)

RB-18 Handling of vulnerabilities, malfunctions and errors – penetration tests

Basic requirement

The cloud provider has penetration tests performed by qualified internal personnel or external service providers at least once a year. The penetration tests are carried out according to documented test methods and include the infrastructure components defined to be critical to the secure operation of the cloud service, which were identified as such as part of a risk analysis. Type, scope, time/period of time and results are documented comprehensibly for an independent third party. Determinations from the penetration tests are assessed and, in case of medium or high criticality regarding the confidentiality, integrity or availability of the cloud service, followed up and remedied. The assessment of the criticality and the mitigating safeguards for the individual determinations are documented.

Supplementary information for the basic requirement

The vulnerabilities should be classified according to the damage potential and specify a period of time for the required response. As guidance, the following classification according to the BSI publication “Ein Praxis-Leitfaden für IS-Penetrationstests” (A practical guide to IS penetration tests) can be used:

- **High:** Immediate response
- **Medium:** Short-term response
- **Low:** Medium-term response
- **Information:** Long-term response

Description of additional requirements (confidentiality and availability)

The tests are carried out every six months. They must always be performed by independent external auditors. Internal personnel for penetration tests may support the external service providers.

RB-19 Handling of vulnerabilities, malfunctions and errors – integration with change and incident management

Basic requirement

Policies and instructions with technical and organisational safeguards for the handling of critical vulnerabilities are documented, communicated and provided according to SA-01. The safeguards are coordinated with the activities of the change management and the incident management.

RB-20 Handling of vulnerabilities, malfunctions and errors – involvement of the cloud customer

Basic requirement

The cloud customer is informed by the cloud provider of the status of the incidents affecting them in a regular and an appropriate form that corresponds to the contractual agreements or is involved into corresponding remedial actions. As soon as an incident was remedied from the cloud provider’s point of view, the cloud customer is informed of the safeguards taken. This information is sufficiently detailed so that the cloud customer can use it in their security management.

RB-21 Handling of vulnerabilities, malfunctions and errors – check of open vulnerabilities

Basic requirement

The IT systems which the cloud provider uses for the development and rendering of the cloud service are checked automatically for known vulnerabilities at least once a month. In the event of deviations from the expected configurations (for example, the expected patch level), the reasons for this are analysed in a timely manner and the deviations remedied or documented according to the exception process (see SA-03).

Supplementary information for the basic requirement

In contrast to the penetration tests (see RB-18) which are performed manually and according to an individual scheme, the checking for open vulnerabilities is carried out automatically using so-called vulnerability management tools.

Description of additional requirements (confidentiality)

Upon customer request, the cloud provider informs the cloud customer of open vulnerabilities in an appropriate form. The open vulnerabilities are remedied promptly without exception.

RB-22 Handling of vulnerabilities, malfunctions and errors – system hardening

Basic requirement

System components which are used for the rendering of the cloud service are hardened according to generally established and accepted industry standards. The hardening instructions used are documented as well as the implementation status.

Description of additional requirements (confidentiality)

Upon request, the cloud customer must be informed of the standards used and the safeguards taken to harden the system components.

RB-23 Segregation of stored and processed data of the cloud customers in jointly used resources

Basic requirement

Data is separated securely and strictly on jointly used virtual and physical resources (storage network, memory) according to a documented concept in order to guarantee the confidentiality and integrity of the stored and processed data.

Supplementary information for the basic requirement

A technical segregation (separation) of stored and processed data of the cloud customers in jointly used resources can be achieved by firewalls, access lists, tagging (identification of the data), VLANs, virtualisation and safeguards in the storage network (e. g. LUN Masking). If the appropriateness and effectiveness of the segregation cannot be assessed with sufficient certainty (e. g. due to a complex implementation), evidence can also be demonstrated by audit results of expert third parties (e. g. penetration tests for the validation of the concept). The segregation of transmitted data is the subject of control KOS-05.

Description of additional requirements (confidentiality)

Resources in the storage network (Storage) are segmented by secure zoning (LUN Binding and LUN Masking).

5.7 Identity and access management

Objective: Securing the authorisation and authentication of users of the cloud provider (usually privileged user) and the cloud customer in order to prevent unauthorised access.

IDM-01 Policy for system and data access authorisations

Basic requirement

A role and rights concept based on the business and security requirements of the cloud provider as well as a policy for the management of system and data access authorisations are documented, communicated and provided according to SA-01 and address the following areas:

- Granting and change (provisioning) of data access authorisations on the basis of the "least-privilege principle" and as is necessary for performing the required tasks ("need-to-know principle")
- Separation of functions between operative and controlling functions (also referred to as "separation of duties")
- Separation of functions in the administration of roles, approval and granting of data access authorisations
- Regular review of granted authorisations
- Withdrawal of authorisations (de-provisioning) in case of changes to the employment relationship
- Requirements for the approval and documentation of the management of system and data access authorisations

IDM-02 User registration

Basic requirement

System access authorisations for users under the responsibility of the cloud provider (internal and external employees) are granted in a formal procedure. Organisational and/or technical safeguards make sure that unique user IDs which clearly identify each user are granted.

Description of additional requirements (confidentiality)

The cloud provider offers self- service options for cloud customers in order to be able to grant user IDs independently.

IDM-03 Granting and change (provisioning) of data access authorisations

Basic requirement

Granting and change of data access authorisations for users under the responsibility of the cloud provider comply with the policy for the management of system and data access authorisations. Organisational and/or technical safeguards make sure that the granted access authorisations meet the following requirements:

- Data access authorisations comply with the "least-Privilege principle".
- When granting data access authorisations, only access authorisations necessary to perform the corresponding tasks should be granted ("need-to-know principle").
- Formal approval is given by an authorised person, before the data access authorisations are set up (i. e. before the user can access data of the cloud customers or components of the shared IT infrastructure).
- Technically assigned data access authorisations do not exceed the formal approval.

Description of additional requirements (confidentiality)

The cloud provider offers self-service options for cloud customers in order to be able to grant and change user data access authorisations independently.

IDM-04 Withdrawal of authorisations (de-provisioning) in case of changes to the employment relationship

Basic requirement

Data access authorisations of users under the cloud provider's responsibility (internal and external employees) are withdrawn in the case of changes to the employment relationship (dismissal, transfer, longer period of absence/sabbatical/parental leave) promptly, but 30 days after its coming into force at the latest and/or suspended temporarily. Any access is deactivated completely as soon as the employment relationship has expired.

IDM-05 Regular review of data access authorisations

Basic requirement

Data access authorisations of users under the cloud provider's responsibility (internal and external employees) are reviewed at least once a year in order to adjust them promptly to changes to the employment relationship (dismissal, transfer, longer period of absence/sabbatical/parental leave). The review is performed by persons authorised to do so from corresponding part of the cloud provider, who are able to review the appropriateness of the granted authorisations due to their knowledge of the responsibilities. The review as well as the adjustments to the authorisations are documented comprehensibly.

Description of additional requirements (confidentiality)

Administrative authorisations are checked at least every six months.

IDM-06 Administrator authorisations

Basic requirement

Granting and change of data access authorisations for internal and external users with administrative or extensive authorisations under the responsibility of the cloud provider comply with the policy or the management of system and data access authorisations (see IDM-01) or a separate policy. The authorisations are granted in a personalised manner and as is necessary for performing the corresponding tasks ("need-to-know principle"). Organisational and/or technical safeguards make sure that granting these authorisations does not result in undesired, critical combinations which violate the principle of the separation of duties (e. g. assigning authorisations for the administration of both the database and the operating system). If this is not possible in certain selected cases, appropriate, compensating controls are established in order to identify any misuse of these authorisations (e. g. logging and monitoring by an SIEM (security information and event management) solution).

IDM-07 Non- disclosure of authentication information

Basic requirement

Secret authentication credentials (e. g. passwords, certificates, security token) is assigned to internal and external users of the cloud provider or cloud customer, provided that this is subject to organisational or technical procedures of the cloud provider, in a proper organised procedure which ensures the confidentiality of the information. If it is assigned initially, it is valid only temporarily, but not longer than 14 days. Moreover, users are forced to change it when using it for the first time. Access of the cloud provider to the authentication information of the cloud customer is strictly regulated, communicated with the cloud customer and only takes place if it is necessary to perform the corresponding tasks ("need-to-know principle"). Access is documented and reported to the cloud customer.

Description of additional requirements (confidentiality)

The users sign a declaration in which they assure that they will treat personal (or shared) authentication information confidentially and keep it private (within the members of the group).

IDM-08 Secure login methods

Basic requirement

The confidentiality of the login information of internal and external users under the cloud provider's responsibility is protected by the following safeguards:

» Identity check by trusted procedures

» Use of recognised industry standards for the authentication and authorisation (e. g. multi-factor authentication, no use of jointly used authentication information, automatic expiry)

» Multi-factor authentication for administrators of the cloud provider (e. g. using a smart card or biometric characteristics) is absolutely necessary

IDM-09 Handling of emergency users

Basic requirement

The use of emergency users (for activities which cannot be carried out with personalised, administrative users, see IDM-06) is documented, to be justified and requires the approval by an authorised person, which takes the principle of the separation of functions into account. The emergency user is only activated as long as it is necessary to perform the corresponding tasks.

Supplementary information for the basic requirement

The approval can also be granted subsequently provided that this is justified.

Description of additional requirements (confidentiality)

At least once a month, the activations of the emergency users and the corresponding approvals are compared manually. Irregularities are examined in order to determine any misuse of these users and to avoid this in the future. The activities of the emergency users are logged in an audit-proof manner. The logging is sufficiently detailed so that an expert third party is able to comprehend the activities.

IDM-10 System-side access control

Basic requirement

Access to information and application functions is limited by technical safeguards with which the role and rights concept is implemented.

IDM-11 Password requirements and validation parameters

Basic requirement

Security parameters on the network, operating system (host and guest), database and application level (where relevant to the cloud service) are configured appropriately to avoid unauthorised access. If no two-factor authentication or use of one-time passwords is possible, the use of secure passwords on all levels and devices (including mobile devices) under the cloud provider's responsibility is forced technically or must be ensured organisationally in a password policy. The targets must at least meet the following requirements:

» Minimum password length of 8 characters

» At least two of the following character types must be included: Capital letters, minor letters, special characters and numbers

» Maximum validity of 90 days, minimum validity of 1 day

» Password history of 6

- Transmission and storage of the passwords in an encrypted procedure that conforms to the state of the art.

Supplementary information for the basic requirement

Security parameters include, for example, the use of secure login methods (see IDM- 08), lock after failed login attempts, no multiple logins with one and the same user, automatic logout/lock after inactivity)

Description of additional requirements (confidentiality)

Automatic controls are implemented, which are based on the following rules:

- There is a lock of 15 minutes after 5 failed login attempts and the waiting time is increased with each failed login attempt.
- Multiple logins of one and the same user are not possible.
- Upon login, there is an automatic lock after 15 minutes of inactivity.
- The minimum password length of privileged users is 14 characters and 8 characters for users without wide-ranging authorisations.
- Capital letters, lower-case letters, special characters and numbers must be included.
- After 90 days, the user is forced to change the password with the next login.
- Password history is 12.

IDM-12 Restriction and control of administrative software

Basic requirement

The use of service programs and management consoles (e. g. for the management of the hypervisor or virtual machines), which allow extensive access to the data of the cloud customers, is restricted to authorised persons. Granting and changes to corresponding data access authorisations comply with the policy for the management of system and data access authorisations. Access is controlled by means of strong authentication techniques, including multi-factor authentication (see KOS-06).

IDM-13 Control of access to source code

Basic requirement

Access to the source code and supplementary information that is relevant to the development of the cloud service (e. g. architecture documentation, test plans) is granted restrictively and monitored in order to prevent unauthorised functions from being introduced and unintended changes from being made.

5.8 Cryptography and key management

Objective: Guaranteeing the appropriate and effective use of cryptography in order to protect the security of information.

KRY-01 Policy for the use of encryption procedures and key management

Basic requirement

Policies and instructions with technical and organisational safeguards for encryption procedures and key management are documented, communicated and provided according to SA-01, in which the following aspects are described:

- Using strong encryption procedures (e. g. AES) and the use of secure network protocols that correspond to the state of the art (e. g. TLS, IPsec, SSH)
- Risk-based regulations for the use of encryption which are compared to schemes for the classification of information and take the communication channel, type, strength and quality of the encryption into account
- Requirements for the secure generation, storage, archiving, retrieval, distribution, withdrawal and deletion of the keys
- Taking the relevant legal and regulatory obligations and requirements into consideration

Supplementary information for the basic requirement

The state of the art regarding strong encryption procedures and secure network protocols is defined in the respectively current version of the following BSI Technical Guidelines:

- BSI TR-02102-1 Cryptographic Mechanisms: Recommendations and Key Lengths
- BSI TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths
  Part 2 – Use of Transport Layer Security (TLS)
- BSI TR-02102-3 Cryptographic Mechanisms: Recommendations and Key Lengths
  Part 3 – Use of Internet Protocol Security (IPSec) and Internet Key Exchange (IKEv2)
- BSI TR-02102-4 Cryptographic Mechanisms: Recommendations and Key Lengths
  Part 4 – Use of Secure Shell (SSH)

KRY-02 Encryption of data for transmission (transport encryption)

Basic requirement

Procedures and technical safeguards for strong encryption and authentication for the transmission of data of the cloud customers (e. g. electronic messages transported via public networks) are established.

Supplementary information for the basic requirement

When transmitting data with normal protection requirements within the cloud provider's infrastructure, encryption is not mandatory provided that the data is not transmitted via public networks. In this case, the non-public environment of the cloud provider can generally be deemed trusted. Strong transport encryption that conforms to the state of the art is currently considered to be the TLS 1.2 protocol in combination with Perfect Forward Secrecy. Furthermore, the BSI Technical Guideline TR-02102-2
Cryptographic Mechanisms: Recommendations and Key Lengths
Part 2 – Use of Transport Layer Security (TLS)
applies in the respectively current version. Using SSL (including version 3.0) is not considered to be a secure procedure.

Description of additional requirements (confidentiality)

If data with higher protection requirements are transmitted, strong encryption must also be implemented within the cloud provider's infrastructure.

KRY-03 Encryption of sensitive data for storage

Basic requirement

Procedures and technical safeguards for the encryption of sensitive data of the cloud customers for the storage are established. Exceptions apply to data that cannot be encrypted for the rendering of the cloud service for functional reasons. The private keys used for encryption are known only to the customer according to applicable legal and regulatory obligations and requirements. Exceptions (e. g. use of a master key by the cloud provider) are based on a controlled procedure and must be agreed upon jointly with the cloud customer.

Supplementary information for the basic requirement

If there is a procedure using a master key by the cloud provider, the appropriateness of the procedure must be examined and compliance verified for a random sample of applications.

KRY-04 Secure key management

Basic requirement

Procedures and technical safeguards for secure key management include at least the following aspects:

- Generation of keys for different cryptographic systems and applications

- Issuing and obtaining public-key certificates

- Provisioning and activation of the keys for customers and third parties involved

- Secure storage of own keys (not those of the cloud customers or other third parties) including the description as to how authorised users are granted access

- Changing or updating cryptographic keys including policies defining under which conditions and in which manner the changes and/or updates are to be realised

- Handling of compromised keys

- Withdrawal and deletion of keys, for example in the case of compromising or staff changes

- Storage of the keys of the cloud users not at the cloud provider (i. e. at the cloud user or a trusted third party)

5.9 Communication security

Objective: Ensuring the protection of information in networks and the corresponding information-processing systems.

■ KOS-01 Technical safeguards

Basic requirement

Based on the results of a risk analysis carried out according to OIS-06, the cloud provider has implemented technical safeguards which are suitable to promptly detect and respond to network-based attacks on the basis of irregular incoming or outgoing traffic patterns (e. g. by MAC spoofing and ARP poisoning attacks) and/or Distributed Denial- of-Service (DDoS) attacks.

Description of additional requirements (confidentiality and availability)

Intrusion prevention/intrusion detection systems (IDS/IPS) are integrated into an overall SIEM system (security information and event management) so that events from IDS/IPS can be correlated with other events in order to be able to initiate the required safeguards (countermeasures) resulting from this. By means of technical safeguards, it is ensured that no unknown (physical or virtual) devices join the (physical or virtual) network of the cloud provider (for example by means of MACSec according to IEEE 802.1X:2010), see IDM-08).

■ KOS-02 Monitoring of connections

Basic requirement

Physical and virtualised network environments are designed and configured in such a way that the connections between trusted and untrusted networks must be restricted and monitored. At defined intervals, it is reviewed whether the use of all services, logs and ports serve a real commercial purpose. In addition, the review also includes the justifications for compensating controls for the use of logs which are considered to be insecure.

■ KOS-03 Cross-network access

Basic requirement

Each network perimeter is controlled by security gateways. The system access authorisation for cross- network access is based on a security assessment on the basis of the customer requirements.

Description of additional requirements (confidentiality)

Each network perimeter is controlled by redundant and high-availability security gateways. The system access authorisation for cross- network access is based on a security assessment on the basis of the customer requirements.

■ KOS-04 Networks for administration

Basic requirement

There are separate networks for the administrative management of the infrastructure and for the operation of management consoles, which are separated logically or physically by the network of the cloud customers and are protected against unauthorised access by means of multi-factor authentication (see IDM-08). Networks which are used for the purposes of the migration or the generation of virtual machines must also be separated physically or logically by other networks.

■ KOS-05 Segregation of data traffic in jointly used network environments

Basic requirement

The data traffic in jointly used network environments is segregated according to documented concept for the logical segmentation between the cloud customers on the network level in order to guarantee the confidentiality and integrity of the data transmitted.

Supplementary information for the basic requirement

If the appropriateness and effectiveness of the logical segmentation cannot be assessed with sufficient certainty (e. g. due to a complex implementation), evidence can also be demonstrated by audit results of expert third parties (e. g. penetration tests for the validation of the concept). The segregation of stored and processed data is the subject of the control. RB-23. For the secure segmentation of jointly used resources for web applications which are provided as SaaS, the session ID in the basic level should:

» be generated randomly and has an adequate entropy of at least 128 Bit (16 characters) in order to withstand the educated guessing of the session ID (for example, by means of a brute-force attack),

» be adequately protected for transmission and client-side storage,

» have limited validity (timeout) which is as short as possible, measured by the requirements for the use of the web application.

Upon successful authentication or change from an insecure communication channel (HTTP), a secure communication channel (HTTPS) should be switched to.

In case of IaaS/PaaS, the requirements for higher protection requirements can be used as guidance in the basic level.

Description of additional requirements (confidentiality)

In the case of IaaS/PaaS, the secure separation is ensured by physically separated networks or by means of strongly encrypted VLANs.

KOS-06 Documentation of the network topology

Basic requirement

The architecture of the network is documented comprehensibly and currently (e. g. in the form of diagrams) in order to avoid errors in the management during live operation and ensure timely restoration according to the contractual duties in the event of damage. Different environments (e. g. administration network and shared network segments) and data flows become apparent from the documentation. Furthermore, the geographical locations, in which the data is stored, are specified.

KOS-07 Policies for data transmission

Basic requirement

Policies and instructions with technical and organisational safeguards in order to protect the transmission of data against unauthorised interception, manipulation, copying, modification, redirection or destruction (e. g. use of encryption) are documented, communicated and provided according to SA-01. The policy and instructions establish a reference to the classification of information (see AM-05).

KOS-08 Confidentiality agreement

Basic requirement

The non-disclosure or confidentiality agreements to be concluded with internal employees, external service providers and suppliers of the cloud provider are based on the requirements of the cloud provider in order to protect confidential data and business details. The requirements must be identified, documented and reviewed at regular intervals (at least once a year). If the review shows that the requirements have to be adjusted, new non-disclosure or confidentiality agreements are concluded with the internal employees, the external service providers and the suppliers of the cloud provider. The non-disclosure or confidentiality agreements must be signed by internal employees, external service providers or suppliers of the cloud provider prior to the start of the contract relationship and/or before access to data of the cloud users is granted.

Supplementary information for the basic requirement

The following should be described in a non-disclosure agreement:

- Which information needs to be handled confidentially
- The terms of the non-disclosure agreement
- What action needs to be taken when the agreement is terminated (i.e. the data media need to be destroyed or returned, for example)
- Who has the rights of ownership to the information
- Which rules and regulations apply to the use and disclosure of confidential information to additional partners, if this is necessary
- The consequences of violating the terms of the agreement

Description of additional requirements (confidentiality)

If adjustments to the non-disclosure or confidentiality agreements result from the review, the internal and external employees of the cloud provider must be informed about this and new confirmations shall be obtained.

5.10 Portability and interoperability

Objective: Allowing the property to be able to securely operate the service on different IT platforms as well as the possibility of securely connecting different IT platforms and terminating the service.

PI-01 Use of public APIs and industry standards

Basic requirement

In order to guarantee the interoperability of cloud services, data regarding documented input and output interfaces and in recognised industry standards (e. g. the Open Virtualization Format for virtual appliances) is available in order to support the communication between different components and the migration of applications.

PI-02 Export of data

Basic requirement

At the end of the contract, the cloud customer can request the data to which they are entitled according to the contractual framework conditions, from the cloud provider and receives them in processable electronic standard formats such as CSV or XML.

PI-03 Policy for the portability and interoperability

Basic requirement

If no individual agreements between the cloud provider and cloud customer regulate the interoperability and portability of the data, policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 in order to ensure the respective requirements and duties of the cloud customer.

PI-04 Secure data import and export

Basic requirement

The cloud provider uses secure network protocols for the import and export of information as well as for the management of the service in order to ensure the integrity, confidentiality and availability of the transported data.

PI-05 Secure deletion of data

Basic requirement

Both when changing the storage media for maintenance purposes and upon request of the cloud customer or the termination of the contract relationship, the content data of the cloud customer, including the data backups and the meta data (as soon as they are no longer required for the proper documentation of the accounting and billing), is deleted completely. The methods used for this (e. g. by overwriting data several times, deletion of the key) prevent the data from being restored via forensic methods.

Supplementary information for the basic requirement

The deletion of meta data and log files is the subject of the requirements RB-11 and RB-13.

5.11 Procurement, development and maintenance of information systems

Objective: Complying with the security targets in case of new developments and procurement of information systems as well as changes.

BEI-01 Policies for the development/procurement of information systems

Basic requirement

Policies and instructions with technical and organisational safeguards for the proper development and/or procurement of information systems for the development or operation of the cloud service, including middleware, databases, operating systems and network components are documented, communicated and provided according to SA-01. The policies and instructions describe at least the following aspects:

- Security in software development methods in compliance with security standards established in the industry (e. g. OWASP for web applications)
- Security of the development environment (e. g. separate development/test/production environments)
- Programming policies for each programming language used (e. g. regarding buffer overflows, hiding internal object references towards users)
- Security in version control

Description of additional requirements (confidentiality)

For the procurement, products which were certified according to the “Common Criteria for Information Technology Security Evaluation” (abbreviated: Common Criteria – CC) according to evaluation level EAL 4 are preferred. If uncertified products are procured although certified products are available, this must be documented and justified.

BEI-02 Outsourcing of the development

Basic requirement

If the development of the cloud service (or parts thereof) is outsourced regarding the design, development, test and/or provision of source code of the cloud service, a high level of security is required. Therefore, at least the following aspects must be agreed upon contractually between the cloud provider and external service providers:

- Requirements for a secure software development process (especially design, development and testing)
- Provision of evidence demonstrating that adequate testing was carried out by the external service provider
- Acceptance test of the quality of the services rendered according to the functional and non-functional requirements agreed upon
- The right to subject the development process and controls to testing, also on a random basis

BEI-03 Policies for changes to information systems

Basic requirement

Policies and instructions with technical and organisational safeguards for the proper management of changes to information systems for the development or operation of the cloud service, including middleware, databases, operating systems and network components are documented, communicated and provided according to SA-01. At least the following aspects are to be taken into account in this respect:

- Criteria for the classification and prioritisation of changes and related requirements for the type and scope of tests to be carried out and permits to be obtained
- Requirements for the notification of affected cloud customers according to the contractual agreements
- Requirements for the documentation of tests as well as for the application and permit of changes
- Requirements for the documentation of changes to the system, operating and user documentation

Supplementary information for the basic requirement

Changes to the existing network configuration must also run through a controlled procedure, since they are necessary for an effective client segregation.

BEI-04 Risk assessment of changes

Basic requirement

The principal of a change performs a risk assessment beforehand. All configuration objects which might be affected by the change are assessed with regard to potential impacts. The result of the risk assessment is documented appropriately and comprehensively.

BEI-05 Categorisation of changes

Basic requirement

All changes are categorised on the basis of a risk assessment (e. g. as insignificant, significant or far-reaching impacts) in order to obtain an appropriate authorisation prior to making the change available to the production environment.

BEI-06 Prioritisation of changes

Basic requirement

All changes are prioritised on the basis of a risk assessment (e. g. as low, normal, high, emergency) in order to obtain an appropriate authorisation prior to making the change available to the production environment.

BEI-07 Testing changes

Basic requirement

All changes to the cloud service are subjected to tests (e. g. for integration, regression, security and user acceptance) during the development and before they are made available to the production environment. The tests are carried out by adequately qualified personnel of the cloud provider. According to the service level agreement (SLA), changes are also tested by the customers (tenants) suitable for this.

BEI-08 Rollback of changes

Basic requirement

Processes are defined in order to be able to roll back required changes as a result of errors or security concerns and restore affected systems or services into its previous state.

BEI-09 Review of proper testing and approval

Basic requirement

Before a change is released to the production environment, it must be reviewed by an authorised body or a corresponding committee whether the planned tests have been completed successfully and the required approvals are granted.

Description of additional requirements (confidentiality and availability)

At least every three months, it is reviewed for an appropriate random sample of changes made to the production environment (i. e. at least 10% of all changes completed during this period of time) whether the internal requirements regarding the proper classification, testing and approval of changes were met.

BEI-10 Emergency changes

Basic requirement

Emergency changes are to be classified as such by the change manager who creates the change documentation before applying the change to the production environment. Afterwards (e. g. within 5 working days), the change manager supplements the change documentation with a justification and the result of the application of the emergency change. This justification must show why the regular change process could not have been run through and what the consequences of a delay resulting from compliance with the regular process would have been. The change documentation is forwarded to the customers concerned and a subsequent release by authorised bodies is obtained according to the contractual agreements.

BEI-11 System landscape

Basic requirement

Production environments are separated physically or logically by non-production environments in order to avoid unauthorised access or changes to the production data. Production data is not replicated in test or development environments in order to maintain their confidentiality.

BEI-12 Separation of functions

Basic requirement

Change management procedures include role-based authorisations in order to ensure an appropriate separation of duties regarding the development, release and migration of changes between the environments.

5.12 Control and monitoring of service providers and suppliers

Objective: Ensuring the protection of information which can be accessed by the service providers and/or suppliers of the cloud provider (subcontractors) and monitoring the services and security requirements agreed upon.

■ DLL-01 Policies for the handling of and security requirements for service providers and suppliers of the cloud provider

Basic requirement

Policies and instructions for ensuring the protection of information accessed by other third parties (e. g. service providers and/or suppliers of the cloud provider), who contribute significant parts to the development or operation of the cloud service, are documented, communicated and provided according to SA-01. The corresponding controls are used to mitigate risks which may result from the potential access to information of the cloud customers. The following aspects are at least to be taken into account for this:

» Definition and description of minimum security requirements with regard to the information processed, which are based on recognised industry standards such as ISO/IEC 27001

» Legal and regulatory requirements, including data protection, intellectual property right, copyright, handling of meta data (see RB-11) as well as a description as to how they are ensured (e. g. site of data processing and liability, see surrounding parameters for transparency)

» Requirements for incident and vulnerability management (especially notifications and collaborations when eliminating malfunctions)

» Disclosure and contractual obligation to the minimum security requirements also to subcontractors if they do not only contribute insignificant parts to the development or operation of the cloud service (e. g. service provider of the computing centre)

The definition of the requirements is integrated into the risk management of the cloud provider. According to requirements OIS-07, they are checked at regular intervals for their appropriateness.

Description of additional requirements (confidentiality and availability)

Subcontractors of the cloud provider are contractually obliged to grant the cloud provider auditing rights regarding the effectiveness of the service-related internal control system as well as with respect to the compliance of the security requirements agreed upon. The subcontractor can also demonstrate evidence by submitting corresponding certificates of independent third parties (e. g. in the form of reports according to ISAE 3402/IDW PS 951). This also includes subcontractors of the subcontractor.

■ DLL-02 Monitoring of the rendering of services and security requirements for service providers and suppliers of the cloud provider

Basic requirement

Procedures for the regular monitoring and review of agreed services and security requirements of third parties (e.g. service providers and/or suppliers of the cloud provider) who contribute essential parts to the development or operation of the cloud service are established. The safeguards include at least the following aspects:

» Regular review of service reports (e. g. SLA reports) if they are provided by third parties

» Review of security-relevant incidents, operational disruptions or failures and interruptions that are related to the service

- Unscheduled reviews after essential changes to the requirements or environment. The essentiality must be assessed by the cloud provider and documented comprehensibly for audits

Identified deviations are subjected to a risk analysis according to requirement OIS-07 in order to effectively address them by mitigating safeguards in a timely manner.

Description of additional requirements (confidentiality and availability)

Interfaces for an automated real-time monitoring of the service (minimum capacity, availability as well as elimination of malfunctions) are established to be able to monitor compliance with the service level agreements agreed upon and to promptly respond to deviations. At least once a year, an audit is performed by independent, external auditors or qualified personnel of the cloud provider in order to review the effectiveness of the controls established at the service provider, which are related to the contract relationship, as well as the security requirements agreed upon. Evidence can be demonstrated, for example in the form of reports according to ISAE 3402/IDW PS 951. The prompt addressing of audit findings is followed up by the cloud provider.

5.13 Security incident management

Objective: Ensuring a consistent and consistent approach regarding the monitoring, recording, assessment, communication and escalation of security incidents.

SIM-01 Responsibilities and procedural model

Basic requirement

Policies and instructions with technical and organisational safeguards are documented, communicated and provided according to SA-01 in order to ensure a fast, effective and proper response to all known security incidents. On the part of the cloud provider, at least the roles listed in OIS-03 must be filled, requirements for the classification, prioritisation and escalation of security incidents defined and interfaces with the incident management and the business continuity management created. In addition to this, the cloud provider has established a “computer emergency response team” (CERT), which contributes to the coordinated solution of specific security incidents. Customers affected by security incidents are informed in a timely manner and appropriate form.

Description of additional requirements (confidentiality)

Instructions are given as to how data of a suspicious system can be collected in the event of a security incident so that it can be used as evidence. Moreover, there are analysis plans for typical security incidents as well as an evaluation method so that the information collected will not lose its evidentiary value during a subsequent legal appraisal.

SIM-02 Classification of customer systems

Basic requirement

All customer systems are classified according to the agreements (SLA) between the cloud provider and cloud customer regarding the criticality for the rendering of services. The assignment of classifications is reviewed regularly as well as after essential changes/events for all customer systems. Deviations are followed up and eliminated in a timely manner. Moreover, the classification shows which parameters regarding the recovery of a system were agreed upon with the cloud customer.

SIM-03 Processing of security incidents

Basic requirement

Events which could represent a security incident are classified, prioritised and subjected to a cause analysis by qualified personnel of the cloud provider or in connection with external security service providers.

SIM-04 Documentation and reporting of security incidents

Basic requirement

After a security incident has been processed, the solution is documented according to the contractual agreements and the report is forwarded for final information or, if necessary, as confirmation to the customers affected.

Description of additional requirements (confidentiality)

The customer can either actively agree to solutions or the solution is agreed upon after a certain period of time has expired. Information about security incidents or confirmed security violations is made available to all affected customers. It is contractually agreed upon between the cloud provider and the cloud customer which data is made available to the cloud customer for their own analysis in the event of security incidents.

SIM-05 Security incident event management

Basic requirement

Logged incidents are centrally aggregated and consolidated (event correlation). Rules for identifying relations between incidents and assessing them according to their criticality are implemented. These incidents are handled according to the security incident management process.

SIM-06 Duty of the users to report security incident to a central body

Basic requirement

The employees and external business partners are informed of their duties. If necessary, they agree to or commit themselves contractually to promptly report all security events to a previously specified central body. Furthermore, information is provided that “incorrect notifications” of events which have not turned out to be incidents afterwards, do not have any negative consequences for the employees.

SIM-07 Evaluation and learning process

Basic requirement

Mechanisms are in place to be able to measure and monitor the type and scope of the security incidents as well as to report them to supporting bodies. The information gained from the evaluation is used to identify recurring incidents or incidents involving significant consequences and to determine the need for advanced safeguards.

Supplementary information for the basic requirement

Supporting bodies can be external service providers or government agencies (in Germany for instance the Federal Office for Information Security (BSI)).

5.14 Business continuity management

Objective: Strategic establishment and control of a business continuity management (BCM). Planning, implementing and testing business continuity concept as well as incorporating safeguards in order to ensure and maintain operations.

BCM-01 Top management responsibility

Basic requirement

The top management (and/or a member of the top management) is specified as the process owner of the business continuity and contingency management and bears the responsibility for the establishment of the process in the company and compliance with the policies. They must ensure that adequate resources are made available for an effective process. Members of the top management and persons in other relevant leadership positions demonstrate leadership and commitment with respect to this topic, for example by asking and/or encouraging the employees to actively contribute to the effectiveness of the business continuity and contingency management.

BCM-02 Business impact analysis policies and procedures

Basic requirement

Policies and instructions for determining impacts of possible malfunctions of the cloud service or company are documented, communicated and provided according to SA-01.

At least the following aspects are taken into consideration:

- Possible scenarios based on a risk analysis (e. g. loss of personnel, failure of building, infrastructure and service providers)
- Identification of critical products and services
- Identification of dependencies, including the processes (incl. the resources required for this), applications, business partners and third parties
- Identification of threats to critical products and services
- Determination of consequences resulting from planned and unplanned malfunctions and changes over time
- Determination of the maximum acceptable duration of malfunctions
- Determination of the priorities for the restoration
- Determination of time-limited targets for the recovery of critical products and services within the maximum acceptable period of time (recovery time objective, RTO)
- Determination of time-limited targets for the maximum acceptable period of time during which data is lost and cannot be restored (recovery point objective, RPO)
- Estimation of the resources required for recovery

BCM-03 Planning business continuity

Basic requirement

Based on the business impact analysis, a uniform framework for planning the business continuity and business plan is introduced, documented and applied in order to ensure that all plans (e. g. of the different sites of the cloud provider) are consistent. The planning depends on established standards which is documented comprehensibly in a "statement of applicability". Business continuity plans and contingency plans take the following aspects into consideration:

- Defined purpose and scope by taking the relevant dependencies into account

- Accessibility and comprehensibility of the plans for persons who have to take action in line with these plans
- Ownership by at least one appointed person who is responsible for review, updating and approval
- Defined communication channels, roles and responsibilities including the notification of the customer
- Restoration procedures, manual temporary solutions and reference information (by taking the prioritisation into account for the recovery of cloud infrastructure components and services as well as orienting to customers)
- Methods used for the implementation of the plans
- Continuous improvement process of the plans
- Interfaces with the security incident management

BCM-04 Verification, updating and testing of the business continuity

Basic requirement

The business impact analysis as well as the business continuity plans and contingency plans are verified, updated and tested at regular intervals (at least once a year) or after essential organisational or environment-related changes. The tests also involve affected customers (tenants) and relevant third parties (e. g. critical suppliers). The tests are documented and results are taken into account for future business continuity safeguards.

Supplementary information for the basic requirement

Tests take place primarily on the operative level and are addressed to operative target groups. These modules include, for example:

- Test of the technical preventive measures
- Function tests
- Plan review

Drills also take place on the tactical and strategic level. These modules include, for example:

- Tabletop exercise
- Crisis team exercise
- Command post exercise
- Communication and alarm exercise
- Simulation of scenarios
- Full scale exercise

After a drill has been performed:

- Review and possible adjustment of the existing alert plan

Description of additional requirements (availability)

In addition to the tests, drills are also carried out, which are, among other things, based on scenarios resulting from security incidents that have already occurred in the past.

BCM-05 Supply of the computing centres

Basic requirement

The supply of the computing centres (e. g. water, electricity, temperature and moisture control, telecommunications and Internet connection) is secured, monitored and is maintained and tested at regular intervals in order to guarantee continuous effectiveness. It has been designed with automatic fail-safe mechanisms and other redundancies. Maintenance is performed in compliance with the maintenance intervals and targets recommended by the suppliers as well as only by personnel authorised to do so. Maintenance protocols including any suspected or detected deficiencies are stored for the duration of the period of time previously agreed upon. After this period of time has expired, the maintenance protocols are destroyed properly and permanently.

Description of additional requirements (availability)

Simulated failures of the supply of computing centres are integrated into the drills (see BCM-03).

5.15 Security check and verification

Objective: Checking and verifying that the information security safeguards are implemented and carried out in accordance with the organisation-wide policies and instructions.

■ SPN-01 Notification of the top management

Basic requirement

The top management is informed of the status of the information security on the basis of security checks by means of regular reports and is responsible for the prompt elimination of determinations resulting from them.

■ SPN-02 Internal audits of the compliance of IT processes with internal security policies and standards

Basic requirement

Qualified personnel (e. g. internal revision) of the cloud provider or expert third parties commissioned by the cloud provider audit the compliance of the internal IT processes with the corresponding internal policies and standards as well as the legal, regulatory and statutory prescribed requirements relevant to the cloud service on an annual basis. The deviations identified are prioritised and, depending on their criticality, safeguards for their elimination are defined, followed up and implemented in a timely manner.

Description of additional requirements (confidentiality and availability)

The audit is carried out at least every six months. The audit also includes the compliance with the requirements of C5.

SPN-03 Internal audits of the compliance of IT systems with internal security policies and standards

Basic requirement

At least on an annual basis, qualified personnel (e. g. internal revision) of the cloud provider or expert third parties commissioned by the cloud provider audit the compliance of the IT systems, provided that they are completely or partially in the cloud provider's area of responsibility and are relevant to the development or operation of the cloud service, with the corresponding internal policies and standards as well as the legal, regulatory and statutory prescribed requirements relevant to the cloud service. The deviations identified are prioritised and, depending on their criticality, safeguards for their elimination are defined, followed up and implemented in a timely manner.

Description of additional requirements (confidentiality and availability)

Upon request of the cloud customer, the cloud provider provides information of the results, impacts and risks of these audits and assessments in an appropriate form. The cloud provider commits their subcontractors to such audits, asks for the submission of the audit reports in the same intervals and uses them for their own audits.

5.16 Compliance and data protection

Objective: Avoiding violations against statutory or contractual duties with respect to information security.

COM-01 Identification of applicable legal, contractual and data protection requirements

Basic requirement

Legally, regulatory and statutory prescribed requirements, as well as the procedure to comply with these requirements and regulations must be identified, documented and updated regularly by the cloud provider for the cloud service related to the respective application.

Supplementary information for the basic requirement

The documentation of the cloud provider may, among other things, refer to the following regulatory requirements:

- Generally accepted accounting principles [German Commercial Code] or IFRS [International Financial Reporting Standards])
- Requirements regarding data access and the auditability digital documents (in Germany e. g. according to GDPdU [German principles of data access and auditability of digital records)
- Requirements for the protection of personal data (e. g. according to BDSG [German Federal Data Protection Act] or EU Data Protection Directive)
- Requirements of the government (in Germany e. g. according to BSIG [BSI Act] or AktG [German Public Companies Act])

COM-02 Planning independent, external audits

Basic requirement

Independent audits and assessments of systems or components which contribute to the rendering of the cloud services are planned by the cloud provider in such a way that the following requirements are met:

- There is only read access to software and data.
- Activities which might impair the availability of the systems or components and thus result in a violation of the SLA are carried out outside regular business hours and/or not at load peak times.
- The activities performed are logged and monitored.

Description of additional requirements (availability)

The cloud provider has taken precautions for unscheduled audits.

COM-03 Carrying out independent, external audits

Basic requirement

Audits and assessments of processes, IT systems and IT components, provided that they are completely or partially in the cloud provider's area of responsibility and are relevant to the development or operation of the cloud service, are carried out by independent third parties (e. g. certified public auditor) at least once a year in order to identify non-conformities with legally, regulatory and statutory prescribed requirements. The deviations identified are prioritised and, depending on their criticality, safeguards for their elimination are defined, followed up and implemented in a timely manner.

Description of additional requirements (confidentiality and availability)

Upon request of the cloud customer, the cloud provider provides information of the results, impacts and risks of these audits and assessments in an appropriate form. If necessary, unscheduled audits can be carried out by independent third parties.

5.17 Mobile device management

Objective: Guaranteeing security when using mobile terminal devices in the cloud provider's area of responsibility for the access to IT systems in order to develop and operate the cloud service.

MDM-01 Policies and procedures for the risk minimisation of access via the cloud provider's mobile terminal devices

Basic requirement

Policies and instructions with technical and organisational safeguards for the proper use of mobile terminal devices in the cloud provider's area of responsibility, which allow access to IT systems for the development and operation of the cloud service, are documented, communicated and provided according to SA-01. These policies and instructions include at least the following aspects, insofar as they are applicable to the cloud provider's situation:

» Encryption of the devices and data transmission

» Increased access protection

» Extended identity and authorisation management

» Ban on jailbreaking/rooting

» Installation only of approved applications from "App Stores" classified as trusted

» Bring your own device (BYOD) minimum requirements for private terminal devices

Description of additional requirements (confidentiality and availability)

Central management and monitoring is performed by means of MDM solutions, including a possibility for remote deletion. A site plausibility check of the access is carried out. An inventory list of mobile terminal devices with access to the cloud service (among other things, with information of the operating system and patch status, assigned employees, approval regarding BYOD) is maintained (see AM-01).

Imprint

Published by
Federal Office for Information Security
Godesberger Allee 185–189
D-53175 Bonn
Email: cloudsecurity@bsi.bund.de
Internet: www.bsi.bund.de/EN/C5

Source
Federal Office for Information Security
Godesberger Allee 185–189
D-53175 Bonn
Phone: +49 (0) 22899 9582-0
Fax: +49 (0) 22899 9582-5400

Last updated
September 2017

Printed by
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
63086 Frankfurt am Main
Internet: www.zarbock.de

Content and editing
Federal Office for Information Security

Image credits
Title: Fotolia

Item number
BSI-Cloud17/202e

This brochure is part of the Federal Office for Information Security's public relations work. It is provided free of charge and is not intended for sale.

www.bsi.bund.de