



Bundesamt
für Sicherheit in der
Informationstechnik



IT Security Guidelines

IT-Grundschutz in brief






Dr. Udo Helmbrecht
President of the Federal Office for Information Security (BSI)

Work and business processes are increasingly based on IT solutions. For this reason, the security and reliability of information and communications technology gains all the more importance. The right IT security concept can assist you in building a solid basis for a level of IT security you can rely on. These IT Security Guidelines are designed to help you with this, providing a compact overview of the most relevant security safeguards. Using practical examples we draw your attention to the risks and illustrate the necessary organisational, infrastructural and technical safeguards. Checklists will assist you in analysing your own situation.

One thing is sure: Security can be achieved without a huge IT budget.

A handwritten signature in black ink, reading 'U. Helmbrecht'.



The "IT Security Guidelines" provide a compact overview of the most important organisational, infrastructural and technical IT security safeguards . They are aimed at IT managers and administrators in small and medium-sized companies as well as in public agencies.

Bundesamt für Sicherheit in der Informationstechnik
(Federal Office for Information Security)

Referat 114 IT-Sicherheitsmanagement und IT-Grundschutz
(Section 114 IT Security Management and IT-Grundschutz)

Postfach 20 03 63
(PO Box 20 03 63)

53133 Bonn GERMANY
Phone: +49 (0)3018 9582-5369

E-Mail: gshb@bsi.bund.de

Internet: <http://www.bsi.bund.de/gshb>

© Bundesamt für Sicherheit in der Informationstechnik 2007

Table of Contents

1	Introduction	5
2	IT security in focus	6
3	Important concepts relating to IT security	8
4	Regulations and legal requirements in Germany	9
5	How not to do it: some warning examples	10
6	The most common failures to act	13
7	Essential security safeguards	17
8	The BSI's IT-Grundschutz methodology	36
9	Standards and certification of one's own IT security	40
10	Annex	42

1 Introduction

In today's information society, life without information and communications technology is almost inconceivable. For this reason, the protection of IT environments is gaining more and more importance. Changed legal requirements are also contributing to a higher awareness for IT security topics: directors are now personally responsible for omissions and inadequate risk prevention.

In practice, however, it is usually difficult to achieve and maintain a satisfactory level of security. The reasons for this are manifold: lack of resources, tight budgets and, last but not least, the increasing complexity of IT systems. A wide range of IT security products and consultants offer quite different solutions. Even experts find it difficult to maintain an overview.

The Federal Office for Information Security (BSI) has been offering information and assistance on all aspects of IT security for many years. The BSI's IT-Grundschutz approach together with the IT-Grundschutz Catalogues has become the most comprehensive standard work on IT security. This approach, which was introduced by the BSI in 1994 and has been further developed ever since, provides both a methodology for setting up a management system for information security and a comprehensive basis for assessing risk, monitoring the existing IT security level and implementing appropriate IT security. The IT-Grundschutz Catalogues are used by numerous companies and public agencies as the basis on which to build their own catalogues of safeguards. In line with developments in information technology, the requirements for IT security have become more and more complex and comprehensive. For this reason, small and medium-sized organisations with limited financial and personnel resources in particular need an introduction to the subject that is easy and fast to implement.

These guidelines are intended to satisfy this need, providing a compact and easily understandable overview of the most relevant security safeguards. The focus is on organisational safeguards and on illustrating threats through practical examples. Technical details have deliberately been avoided.

In short, anyone who consequently implements the recommendations made in these guidelines or who uses them to draw up service contracts with IT service providers is already building a solid foundation for a reliable level of IT security.

2 IT security in focus

Security is a basic need of human beings, and hence of our society. Especially in the era of globalisation, rising mobility and growing dependence on information and communication technology by the industrial nations, this need for security is becoming ever more pronounced.

Increased vulnerability and the threat of massive financial damage as a result of IT problems are augmenting the pressure to take action to prevent damage and minimise the residual risk through active IT security management. Responsibility is not confined to the IT departments concerned. On the contrary, security is a managerial issue. And, moreover, the legislator has recognised this. Various laws and regulations now make directors personally responsible should they fail to take the required action.

It is widely believed that IT security safeguards necessarily entail high investment in security technology and that their implementation requires highly skilled personnel. However, this is not the case. The main ingredients of success are common sense, well thought out organisational procedures and reliable, well informed staff who independently and expertly observe security requirements in a disciplined manner. The creation and implementation of an effective IT security concept therefore need not necessarily be expensive. The most effective safeguards are surprisingly simple and often do not actually cost anything!

Another widely held misconception concerns the actual protection requirement. Often one hears remarks like:

"Nothing ever happened to us so far" This is a brave statement to make. It is perfectly possible that there have been security incidents before but that they went unnoticed.

"Why would anyone want to attack us, our data is not that confidential." In most cases, such a view is too superficial. When taking a closer look at damage scenarios, it soon becomes clear: some of the data that is processed can be misused in a variety of ways if in the wrong hands.

"Our network is secure." Often the capabilities of potential aggressors are underestimated. Moreover, even an experienced network or security specialist cannot know everything and occasionally makes mistakes. External reviews nearly always uncover serious vulnerabilities and are a good protection against "operational blindness".

"Our staff can be trusted." A variety of statistics paint a different picture: the majority of security breaches are caused by insiders. These security breaches do not always involve malicious intent. Serious damage can also be occasioned by mistake, overzealousness or curiosity coupled with a lack of awareness of the problem.

Everyone has to recognise that security is not a static condition but an ongoing process. Therefore you should constantly ask yourself the following questions:

- ▶ If confidential information from your organisation were to fall into the hands of third parties, how could it be improperly used?
- ▶ What would be the consequences for you if important information were modified, for example, during data transmission or on your server? The cause does not need to be malicious intent on the part of unknown third parties but could also be a technical failure.
- ▶ What would happen if vital computers or other IT components in your organisation suddenly failed and could no longer be used for an extended period (days, weeks etc.)? Would everyone be able to continue their work? How extensive could the damage be?

A well thought out IT security concept, if implemented, will bring additional benefits over time on top of the gain in security. IT managers frequently observe the following "side-effects":

The workforce is more reliable, the quality of work is better.

The active experience of IT security promotes an organisational culture in which responsible action, customer orientation and identification with the organisation's goals are firmly anchored.

Competitive advantages

Proof of IT security creates trust on the part of customers and other business partners and is also increasingly demanded by them.

Maintenance work on IT systems takes a lot less time. Administrators work more effectively.

Administrators and users get to know their systems better. IT systems are well documented, and this in turn makes administrative work, planning, installation of software and troubleshooting easier.

Moreover, a good IT security concept avoids some problems from which administrators normally suffer. Different users use different programs for the same purpose, different operating systems have to be supported, different versions of the same software are in service, every user has his or her own set of permissions, users run their own, private software and configure their workstations themselves, without having the necessary expertise. Central administration of this "computer chaos" is virtually impossible. Every computer has to be individually analysed and maintained, increasing the effort required.

3 Important concepts relating to IT security

There are **three fundamental values of IT security**: confidentiality, availability and integrity.

Confidentiality: information that is confidential must be protected against unauthorized disclosure.

Availability: services, IT system functions, data and information must be available to users as required.

Integrity: data must be complete and unaltered. In information technology, the term "information" is used to refer to "data" to which, depending on the context, certain attributes, such as the author or time of creation, can be assigned. The loss of integrity of information can therefore mean that this data has been altered without authorisation, that information relating to the author has been falsified or the date of creation has been tampered with.

Some other terms frequently used are:

Authentication: When a person logs in on a system, the system runs a check in an authentication process to verify the identity of the person. The term is also used when the identity of IT components or applications is tested.

Authorisation: Authorisation is the process of checking whether a person, an IT component or an application is authorised to perform a specific action.

Data protection: Data protection refers to the protection of personal data against misuse by third parties (should not be confused with data security).

Data security: Data security refers to the protection of data in respect of requirements on its confidentiality, availability and integrity. An alternative term for this is "IT security".

Data backup: Data backup involves making copies of existing data to prevent its loss.

Penetration testing: Penetration testing is a directed, normally simulated attack on an IT system. It is used as a test of the effectiveness of existing security safeguards.

Risk assessment or analysis: A risk analysis provides information on the probability of the occurrence of a damaging event and what negative consequences the damage would have.

Security policy: In a security policy the security objectives and general security safeguards are formulated in the sense of the official regulations of a company or a public authority. Detailed security safeguards are contained in a more comprehensive security concept.

4 Regulations and legal requirements in Germany

Imagine the situation in which data held in your organisation becomes public, data is maliciously or accidentally destroyed in such a way that it cannot be restored. Or mass e-mails infected with computer viruses are sent out from your organisation. What consequences would this have on the organisation and the persons responsible?

Overview of the legal requirements regarding IT security

During the last few years, several statutory requirements have come into force, as a result of which the directors of a company have a duty to act and are held liable on matters of IT security. These statutory requirements apply both to public and private limited companies. This is not yet common knowledge.

In this connection reference is always made to the Control and Transparency in Business Act (**KonTraG**). The KonTraG is an act that supplements or amends several other pieces of legislation such as the German Commercial Code and the German Stock Corporation Act. In particular, the requirement for risk management for limited companies, i.e. both for public and private limited companies, was not covered by previous regulations.

Specifically you could be affected by the following provisions:

The **German Stock Corporation Act** (Aktengesetz, AktG) lays down that a director is personally liable if he fails to monitor developments that could constitute a risk to the company in the future via risk management and does not take appropriate preventive safeguards (S.91 para. 2 and S.93 para. 2 AktG).

Under the **Limited Liability Companies Act** (GmbH-Gesetz, GmbHG), the directors of a private limited company have a duty to exercise the "circumspection of a responsible businessman" (S.43 para. 1 GmbHG).

The directors' duties specified in the German Stock Corporation Act also apply within the framework of the **Commercial Code** (Handelsgesetzbuch, HGB) (S.317 para. 4 HGB). Moreover, the German Commercial Code places an obligation on the auditors to check "whether the risks of future developments are accurately presented" (S.317 para. 2 HGB).

To a layperson, some of the above provisions may sound quite general and woolly. In fact, however, they form the basis for concrete obligations to ensure a reasonable level of IT security in one's own company. IT security incidents can cause massive financial damage and, in the worst case, can put at risk the continued existence of an enterprise.

For certain professional groups such as doctors and lawyers and members of the caring professions, the **German Penal Code** (Strafgesetzbuch, StGB) contains special provisions which even provide for prison sentences where confidential details of patients or clients are published without their consent (S.203 StGB). Negligent handling of information technology may already qualify for such a sentence.

A number of laws deal with consumer protection concerns. The use of information technology, the Internet or telecommunications services is in places regulated to the tiniest detail. Pertinent are here, for example, the Use of Teleservices Act, the Telecommunications Act, the German Interstate Treaty on Media Services, copyright legislation and various EU directives.

The handling of personal data is regulated in the national and state data protection legislation, the Act Concerning Data Protection in Teleservices, the Telecommunication Data Protection Regulation (1991) and to some extent in the legislation already mentioned.

Banks now have an obligation when granting credit to consider any IT risks of the borrower, and this has a direct effect on the conditions offered (keyword: Basle II).

As you can see, there are plenty of reasons why it is important to concern yourself in depth with the subject of IT security. For your own security, get an expert to explain your own legal situation to you!

5 How not to do it: some warning examples

Scenario 1: "No Backup"

A law office operates a small network with a central server, on which all data is stored. The server has a tape drive, to which backup copies are saved at regular intervals. The administrator keeps the backup tapes in a locked cabinet in his office. One day a hard disk fault causes the server to fail and the data needs to be restored from the backup tape. However, it transpires that the tape drive had evidently developed a fault some time ago and no data has been written to the backup tapes. The only backup tape still usable is over five years old. As a result, all the data for the last few years has been lost.

The administrator has overlooked another potential danger in planning the backups: even if the tape drive had worked properly, in the event of a fire or similar catastrophe, not only would the original data have been destroyed but also the backup media in his cabinet!

Safeguards

- ▶ Regular checking of backup tapes
- ▶ Test and practise restoring data
- ▶ Store backup tapes outside one's own office accommodation, for example, in a safe-deposit box in a bank.

Scenario 2: "Infection by computer viruses"

A company uses virus protection programs right across the organisation. However, the virus definitions are only sporadically updated, for example, as part of an operating system update. One day the IT department receives a virus warning regarding a new e-mail virus that is spreading like wildfire over the Internet to more and more recipients. However, the company does not have any automated update mechanism that would enable all the virus protection programs to be updated with the new virus definitions at breakneck speed. By way of emergency safeguard, the mail servers are disconnected from the Internet. However, the virus has already infiltrated the internal network and its further dissemination cannot be prevented. As the virus deletes Office documents, every computer has to be taken off the network and shut down until the IT managers can gradually install a virus definitions update on every machine and laboriously "disinfect" any computers already infected. The entire IT operation comes to a virtual standstill for several days. Significant financial damage is caused by the destruction of data, delays in order processing and lost working time. Shortly after completing this work, the first variants of the virus, which are not yet detected by the carefully updated virus protection program, appear on the Internet. The entire exercise has to be repeated all over again.

Safeguards

- ▶ Create an update concept for security updates
- ▶ Do not forget "IT islands" within the organisation (e.g. notebooks and test computers)

Scenario 3: "Sudden departure of the administrator"

A medium-sized company has an administrator who for years has had sole responsibility for installing and configuring all the PCs and operating the network. One day the administrator sustains a serious accident and is no longer able to work.

Within a few days problems with the network servers are already mounting: error and warning messages appear, but these are not correctly interpreted by the staff, who do not know what to do. Shortly afterwards several computers stop working and after a failed attempt to reboot them virtually

nothing is working any more. During the search through the administrator's documents that now begins, it becomes apparent that the existing system environment is virtually undocumented. Even administrator passwords have not been recorded. An IT support company called in to provide emergency support is unable to restore the existing system because the passwords are unknown and the documentation is so poor. A laborious investigation is carried out to establish which applications were installed on the servers and where these had stored the data that is important for the company. Additional external specialists need to be called in, for, apart from widely used standard applications, some industry-specific customised solutions are in use which the systems house entrusted with restoring the system has never seen before.

Several weeks go by before everything has been restored and all the systems required for everyday work are functioning in their normal fashion. In the meantime important orders cannot be fulfilled in the company as the information and applications required for this are not available. Including the cost of calling in the external service providers, the damage comes to a six-figure sum. The very survival of the company is under threat. On top of everything else, a suitable replacement must be found for the administrator who is no longer able to work.

Safeguards

- ▶ Document system settings and parameters in detail
- ▶ Record passwords securely
- ▶ Create a contingency plan with instructions on what to do in the event of the most probable damaging events
- ▶ Put in place deputisation arrangements

Scenario 4: "Hacker attack from the Internet"

A psychologist has a practice in a small town. He keeps all his patient records on a PC that is connected to the Internet. He knows his way round his PC and generally installs his software himself. He believes his data is secure as he has to log on to the system with a password. One day the news that confidential patient information has been anonymously published in a local internet discussion forum for the town spreads like wildfire throughout the whole town. The police investigation leads to the psychologist and establishes that the practice PC was totally inadequately protected against third party attacks and was probably the target of a hacker attack. The public prosecutor charges the psychologist with negligence in the handling of confidential patient data. The damage sustained by the patients concerned is enormous and can hardly be quantified.

Safeguards

- ▶ Secure internet access
- ▶ Encrypt confidential data

Scenario 5: "Insider attack"

A small, traditional company has been manufacturing special paints and varnishes using a secret formula for many years. One day an employee in the marketing department leaves and joins a competitor. Six months later the rival company brings some almost identical varnishes out on the market. At first it is not apparent how the secret formula could have left the company as, for security reasons, the development department is not connected either to the intranet or the Internet. The company therefore suspects industrial espionage by the former employee and reports him to the police.

The criminal investigation department is able to prove using appropriate tools that files containing the formula in question had first been stored and then later been deleted on the suspect's PC. Confronted

with these facts, the suspect confesses. It transpires that the development department rooms were not locked at night and could therefore be entered unnoticed by any employee with a key to the building. After work the suspect had found his way to the development department, and with the aid of a boot disk, which meant he could circumvent having to enter a password, he had gained access to the critical computers. His new employer had asked him when he applied for the job whether he had any "valuable additional knowledge from the business environment" that would make him more valuable than other applicants.

Both the thief and also two managers at his new employer's are charged and receive sentences. The two companies settle out of court. Despite this, the first company has largely lost its competitive advantage, resulting in a worsening of its financial position.

Safeguards

- ▶ Secure rooms and buildings against unauthorised access
- ▶ Encrypt important data

6 The most common failures to act

When one analyses typical errors and omissions, company size and industry appear to have little relevance. Using the list below, you can check which specific omissions are relevant in your environment and how this situation should be assessed. The next chapter examines the shortcomings presented once again and shows, using specific safeguards, how you can counter these with only moderate expenditure.

6.1 Inadequate IT security strategy

Security is not regarded as important

Compared with other requirements, such as costs, convenience, extent of functionality etc., security is often only a low priority. Instead, IT security is viewed simply as a cost driver and an obstruction. Especially when it comes to new purchases, the security features of an application or system are frequently neglected or not even considered. There are numerous reasons for this: lack of management support for IT security, inadequate research regarding security aspects, new trends in the industry, marketing considerations or tight budgets etc. Security deficiencies are generally not immediately obvious. Instead, "only" the risk arising from these deficits increases! In the most unfavourable case, necessary security safeguards are continually postponed to the indefinite future, as every time they are assigned a low priority compared with other problems that have surfaced in the meantime.

One example in this connection is the meteoric rise in the number of completely insecure wireless networks, given that the relevant WLAN cards have fallen substantially in price. Excitement over a new technology and the possibility of managing without troublesome wires could cause one to overlook security aspects. In this way, countless companies unintentionally "publish" their confidential data and in some cases offer anyone interested free internet access.

Lack of enduring processes for maintaining the security level

Often security is only created within the context of isolated individual projects. These projects are necessary to initiate specific actions and handle a situation to an appropriate depth. However, frequently people forget to also define reliable processes within the context of such projects that will maintain the results and objectives achieved during the project on a permanent basis. Thus, for example, elaborate vulnerability analyses are carried out and recommendations are made as to which safeguards to implement. But when it comes to implementing them later on, the recommendations are not followed in a consistent fashion. Similarly, when new systems are installed, usually detailed requirements are listed for the secure basic installation. However, experience suggests that the parameter settings undergo constant change during later productive operation. Despite this, checking for compliance with the original requirements is seldom carried out. Examples of this kind are available in abundance. Many of these shortcomings are a feature of poor internal IT security management: sometimes it is unclear who is responsible for security management tasks, sometimes agreed safeguards are not regularly reviewed.

Security objectives are not documented

Many large institutions have a fixed, written security policy and instructions regarding its application. In most small and medium-sized organisations, however, this is not the case. Moreover, many policies are too abstract and allow too much leeway for different interpretations. If policies do exist, frequently not everyone who should know about them does. Often they are not binding in the sense of a policy whose observance is an explicit, recognised requirement in the employment contract. In individual cases this can mean that security breaches go unpunished or are difficult to prosecute.

Lack of control mechanisms or investigation in case of security breaches

Security policies and objectives are only effective if adherence to them can also be monitored. However, frequently there is no such monitoring, for technical, administrative or even legal reasons. Another problem is where employees do not have to face the consequences if they do commit a security breach. Both cases have the effect of encouraging further flouting of the rules, thus increasing the security risk and ending in actual cases of damage.

6.2 Mistakes in the configuration of IT systems

The granting of permissions is not sufficiently restrictive

One of the golden rules of IT security is the “need-to-know principle” which requires that every user (and also every administrator) should only be allowed to access that data and run those programs that they really need for their everyday work. In practice, however, this implies additional administrative and technical effort. Hence most employees have access to a lot of sensitive data and programs that they do not need. As workstation PCs and servers are generally networked with each other in an organisation, without suitable access restrictions it is often possible to access data belonging to other users or on different computers. The people who “own” this data are frequently not aware of this. In this way excessively lax permissions can be abused accidentally, through ignorance or intentionally.

IT systems are poorly configured

In practice, by far the most security loopholes arise from mistakes in administration rather than through software bugs. If the security functionality provided in standard software were to be implemented correctly and in full, the IT security level in the organisation would be a lot higher. The complexity of standard office applications is continually increasing. For administrators, security is only one of many, sometimes competing requirements confronting them in their work. In effect, they are not really in a position to completely avoid incorrect (insecure) parameter settings. Many of those concerned are aware of this dilemma, but without adequate support from their managers no changes are likely to take place.

6.3 Insecure networking and internet connection

Sensitive systems are not adequately sealed off from open networks

As long as information and data are only available on the internal network, the risk posed by security loopholes is restricted to a finite population of potential wrongdoers (the workforce). However, when the system is open to the Internet it must be borne in mind that vulnerabilities can be detected and exploited by anonymous third parties, for example, hackers. The secure connection of existing applications to the Internet requires specific knowledge on the part of the administrators concerned, without which configuration errors can hardly be avoided. Sensitive information, systems and subnets are often not isolated or only inadequately isolated from open networks. Even the existence of a firewall says nothing about the actual state of security. Many IT managers think that a firewall is sufficient to protect their network from the outside world. However, an audit by (external) security specialists will in many cases reveal serious security vulnerabilities.

6.4 Failure to observe security requirements

Security safeguards are ignored for the sake of convenience

The best policy and security functions are to no avail if they are not observed or not used. Confidential documents or e-mails are often not encrypted, even where suitable mechanisms are directly available.

In addition, the requirement for a secure password that is changed at regular intervals or for a password-protected screensaver is regarded as onerous. Passwords are disclosed to any old caller who purports to be a new employee of the IT department and asks "nicely" for the information.

Data, especially on notebooks, is seldom or never backed up, even though those involved are aware of the high risks of losing data. Even if regular data backups are carried out, often these are incomplete or flawed. Where automatic backups are made, often employees do not know what data is backed up, at what intervals and how long the backup media are kept for. Numerous other examples of a similar nature exist and show that even simple security safeguards are doomed to failure if the workforce does not accept the need to carry them out or the safeguards cannot be technically enforced. This applies not only to users but also to administrators. Administrators are only seldom bothered about ensuring that the parameter settings are sufficiently secure. Moreover, they often routinely work logged in under a privileged administrative ID. Even when there is no technical reasons for this, it is more convenient to carry on working under this ID than to log off and then log on again under a normal ID.

Inadequate training of users and administrators

Constant changes in the IT systems and applications used in companies and public bodies necessitate a high degree of self-initiative by those concerned if these systems are to be competently handled. However, learning by trial and error is hardly a suitable way of learning how to adequately master increasingly complex systems, especially if it is not done in a test environment. Manuals are not always available. Often there is no time to read them. Frequently training does not cover the specific requirements of those attending. Moreover, seminars are usually expensive and those attending are not available for their normal duties in their own organisations for the duration of the training. Finally, detailed knowledge of only isolated, selected in-depth areas (e.g. Windows 2000, Lotus Domino or Apache) is seldom sufficient on its own, as it does not take into account interactions between different aspects of all of these systems.

6.5 Poor maintenance of IT systems

Failure to install the available security updates

Often administrators do not install security patches promptly. Much of the damage caused by viruses or worms only becomes apparent some time after the existence of the pest has become known. By this time there are usually security patches available from the various manufacturers. These days security patches are published for most products at frequent intervals. Selection and testing of the patches that are actually relevant in one's own circumstances takes more time. Many administrators therefore prefer to wait until the next regular software update is installed. Such an approach is negligent.

6.6 Careless handling of passwords and security mechanisms

Careless approach to passwords

Most access protection mechanisms continue to be implemented on the basis of password prompting. Problems arise where insecure (e.g. too short or easy to guess) passwords have been chosen. Intrusions into IT systems take place on a daily basis because an attacker has successfully cracked a password, sometimes through systematic trial and error, guessing or spying. The proverbial keeping of the password under the keyboard or in the top drawer of the desk makes it particularly easy for perpetrators with access to office premises to get their hands on sensitive information.

Failure to use existing security mechanisms

Many products are supplied with built in security mechanisms, but for the sake of an easy life, out of mistrust or for compatibility reasons these are not activated or are configured too ineffectively. For example, the available encryption function in wireless networks (WLANs) is used far too infrequently.

6.7 Inadequate protection against intruders and damage by the elements

Offices and IT systems inadequately protected against theft or damage by the elements

Intruders and thieves often have all too easy a time. Windows left ajar overnight, unlocked IT rooms, unsupervised visitors and notebooks left in the car offer a variety of possibilities to uninvited visitors. Usually the loss of data is even more serious than the loss of the hardware itself through theft or vandalism. On the one hand this is difficult to recreate, while on the other hand there is a danger that the thief could misuse confidential data. Catastrophes such as fire or flood may be rare events, but when they do occur the consequences are usually fatal. Fire precaution safeguards, protection against damage by water, and an uninterrupted power supply should therefore be viewed as an important element of IT security.

7 Essential security safeguards

7.1 Systematic approach to IT security

Appropriate attention to IT security

1. IT security aspects must be adequately considered early on in all projects

The requirements for the widest possible range of programs with high functionality, ease of use, low procurement and operating costs as well as IT security are nearly always competing factors. However, it is absolutely essential that IT security aspects are considered right from the start of a project (e.g. when purchasing new software or planning business processes). New technology should not be implemented indiscriminately. It is imperative here that IT security objectives should be unambiguously supported at management level. Security defects that become apparent only later on can have unpleasant consequences. If design or planning errors emerge after the event, often it is inordinately expensive or even impossible to remedy them. Having the courage to make life less convenient or to forego certain functionality can prevent high costs in terms of security incidents and eliminate the need for expensive investment in additional IT security products.

2. Where resources are tight, alternative solution approaches should be considered

Often there are many ways of achieving the same goal. Costly and protracted projects are exposed to a higher risk of being "overturned" due to lack of time, money or changes in the framework conditions. Therefore, alternative approaches with initially more modest objectives should be considered. Several small steps can be implemented more easily than one big one. This too is an aspect of security.

Step-by-step to greater IT security

3. The IT security objectives must be specified in order that appropriate safeguards can be defined.

When considering IT security, the first step is to take stock:

- ▶ What framework conditions apply (legislation, contracts, customer requirements, competitor situation)?
- ▶ What role do IT and IT security play in the company or agency?
- ▶ What valuables need to be protected (expertise, trade secrets, personal data, IT systems)? What potential damaging events are there?

The "assessment of protection requirements" is a necessary part of every security analysis. This should ensure that the defined protection goals and the security safeguards derived from these are reasonable and appropriate to the particular circumstances. As framework conditions can change over time, it is necessary to check at regular intervals whether the rating of protection requirement is still appropriate to the present situation. During the assessment of protection requirements it is helpful to orient oneself to the three fundamental values of IT security, *confidentiality*, *integrity* and *availability*.

4. Suitable controls should be drawn up for every security objective and every associated safeguard

"IT security is an ongoing process." This statement sums up the core problem: most of the tasks associated with IT security have to be repeated regularly. Every safeguard identified should be examined to establish whether it needs to be implemented only once or must be repeated at regular intervals (e.g. regular updating of anti-virus software).

5. An action plan setting out clear priorities as regards security objectives and safeguards should be created

Anyone who has given serious thought to the issue of sensible moves to raise IT security within the organisation will soon find themselves confronted with more tasks than time and financial resources permit. It is therefore necessary to prioritise the identified security objectives and safeguards in a suitable manner. Such prioritisation should also take into account the relationship between cost and benefit.

6. Particularly onerous security requirements should be avoided

If possible, only security objectives which are practical to adhere to and will not be viewed as unrealistic or even annoying by a majority of those affected should be defined. Moreover, it goes without saying that the technical and organisational infrastructure needed to implement objectives and safeguards must be provided. Otherwise there is a danger that the policy as a whole will no longer be taken seriously and will increasingly be disregarded. In case of doubt, the requirements should be scaled down and more emphasis should be placed on observing them. It is also recommended that all safeguards which have a particularly pronounced effect on normal operating methods should be discussed in advance with the users concerned.

7. Responsibilities must be defined

For every identified task it is necessary to specify who is responsible for carrying it out. Similarly, for all generally formulated security policies it should be made clear for which persons these are mandatory: do they affect only permanent staff, a particular department or everyone?

Every person in a position of responsibility needs someone who is authorised to stand in for them when necessary. It is important that such persons are also in a position to perform the tasks they may be required to perform in this capacity. Have they been briefed on the work? Have any necessary passwords been deposited in a safe place for an emergency? Is there any documentation that they need?

8. Existing policies and responsibilities must be known

In surveys of staff in companies, often one finds that existing policies relating to IT security are not known or only partially known. Sometimes people are not even aware of their existence. Steps must therefore be taken to ensure that all those affected are familiar with the latest version of company policy. All staff should know their internal and external points of contact and their competencies. This is not just aimed at ensuring that help is available more quickly to deal with problems. It also prevents staff from allowing themselves to be persuaded or intimidated into disclosing confidential information (e.g. passwords) to unauthorised persons.

Legal considerations are also relevant here, so that in the event of a breach of security punishment does not falter because the guilty party can justifiably claim ignorance. If required, it can be a good idea to make staff confirm in writing their awareness of important policies.

Monitoring and maintaining IT security

9. IT security should be checked regularly

The level of IT security should be monitored and assessed regularly. If an adequate budget is available, consideration should be given to calling in independent experts once a year to check especially critical areas of IT. Thinking ahead is imperative: are there any new security standards or important new technologies? Have the expectations of customers and business partners changed?

10. Existing work routines and security policy should be checked regularly to ensure that they are suitable and efficient

Ongoing optimisation of existing processes and policy is not just a matter for those in charge of IT security. As far as the formulation of security policy is concerned, there are three main dangers: it could be out of date, incomplete or not practicable. If security objectives are to gain acceptance among the workforce they must not be experienced as cumbersome or unreasonable. From this point of view, all work routines that are related to IT security tasks should be critically examined. Personal assessment of work routines by the persons performing those routines is a necessary contribution. If a survey establishes that individual safeguards are not rated as useful, then together the reasons and possibilities for improvement should be investigated.

Further steps

The importance of the next two safeguards depends very much on the size of the company or agency. The more staff are affected, the more necessary and sensible it is to implement them.

11. In the long term, full security management should be set up

A good level of IT security can only be achieved in larger organisations if, step-by-step, full IT security management is established. This includes the aspects contained in the present guidelines, but extends far beyond them. Surveys show that in companies which have full IT security management the number of security incidents is significantly lower.

12. Security policy should be properly documented in a security concept

It is recommended that the security policy of an organisation is documented in writing. Today there are plenty of examples available on the Internet and in the technical literature that can be used freely and adapted to an organisation's particular requirements. Sometimes it proves easier to adopt and tailor

a well structured policy document written by a third party than to rework a set of provisions that has evolved over time, is poorly structured and may contain contradictions.

Experience shows that such policies are easiest to supplement and update when they are carefully divided into several (at least 3) levels of abstraction.

The uppermost and most abstract of these concentrates on general security objectives and essentially is a summary of the salient points of the organisation's philosophy in the matter of IT security. This is only a few pages long, is "suitable for management" and should be approved by senior management.

The second, underlying level contains detailed security objectives, technical requirements and associated safeguards. This should be as detailed as possible without, however, going into product-specific aspects or characteristics, so if there are any changes in the products and IT solutions used, the security objectives will not need to be permanently changed.

The interpretation of the requirements formulated here into specific product settings and mechanisms to be used is contained in the third level. This must be modified as soon as there is a change in a product used. Sadly it is often the case that previously formulated requirements cannot be implemented due to lack of product features or practicability. In that case either the requirements need to be reassessed or another solution must be used. What is clear is that any shortcomings regarding the implementation must be explicitly recorded. All those responsible must be informed so that they can assess the resulting risk.

7.2 Security of IT systems

13. Existing protection mechanisms should be used

A lot of programs that are used in a normal client/server based network for office communications now come with a variety of excellent protection mechanisms. Nearly always vulnerabilities are the result of configuration mistakes or ignorance of the available protection facilities. The security functions and mechanisms implemented by the manufacturer should therefore be analysed, understood and implemented – before existing security requirements are actively not implemented or are implemented only by a circuitous route. In this way security requirements can be technically enforced which otherwise would require willingness to co-operate on the part of the users.

14. Anti-virus software must be used throughout the organisation

It is imperative to employ up-to-date anti-virus software. Viruses can be propagated via data media or over networks (Internet, Intranet). They are also mandatory even for computers that are not connected to the Internet.

It is recommended that e-mail and every communication over the Internet are virus-checked centrally. In addition, every computer should have a local virus protection program that runs permanently (resident) in the background. Usually, it is sufficient to monitor executable files, scripts, macro files etc. only. Nevertheless, it is recommended to have all files scanned at regular intervals (e.g. prior to the daily or monthly backup). This is imperative following infection by a virus.

The latest recommendations and detailed background information is available on the BSI website under the heading "Computer-Viren" (only available in German).

Caution:

Even if your virus protection program is always up-to-date, it still does not offer absolute protection against computer viruses, worms and other malware. You must therefore assume that your system is exposed to new viruses for at least until the manufacturers of anti-virus software have issued appropriate virus signatures. Malicious programs that are propagated over the Internet and are technically designed so that they can infect computers via a vulnerability which has not been eliminated are also dangerous. One well-known example is the "Lovsan" (W32.Blaster.Worm) worm, which exploited a vulnerability in Windows 2000 and Windows XP. This worm could only be fended off with a restrictively configured firewall; e-mail filter software was powerless to protect against it.

15. Data access possibilities should be restricted to the minimum level needed

One of the golden rules of IT security is the "need-to-know principle" which requires that every user (and also every administrator) should only be allowed to access the data and run the programs that they really need for their everyday work. This includes ensuring that information belonging to one department (e.g. sales, development, human resources, management etc.) cannot be automatically accessed by people from other departments, assuming that this information is not necessary for their work. Application programs, especially system administration programs, should likewise be available only to the staff who really need them.

This principle can be implemented without great expense: necessary permissions are combined into suitable authorisation profiles. On this basis, suitable user groups or roles are then defined. The individual permissions of a system user can then be determined by group memberships or by the roles that the user is allowed to assume. Checks as to whether the access rights available to a person still match that person's activity profile or whether restrictions would be appropriate should be carried out at regular intervals. To have a clear picture of access authorisation, one's own network can be examined regularly with suitable tools. This will identify resources which it may be undesirable for any third parties to be able to access. Many suitable tools are available free of charge.

A suitable process for granting permissions for new staff and changed roles and for revoking them for leavers must also exist.

16. Roles and profiles must be assigned to all system users

Access authorizations should not be assigned to individual persons or groups of persons as a hotchpotch of different permissions, since, when large numbers of persons have to be administered, this approach inevitably requires a lot of administrative effort, is highly complex and hence highly susceptible to errors. Virtually all standard applications therefore offer the possibility of defining appropriate authorisation profiles and creating suitable roles with their assistance. Every user (and also

every administrator) is assigned one or more permissible roles which he/she can assume during work. This not only permits simpler (and therefore more secure) authorisation management; it also enables more flexibility, as the same person can assume different roles depending on the particular tasks or activities he/she is presently performing.

17. Administrator privileges should be restricted to the extent necessary

Many system administrators work under an administrative role which is subject to virtually no restrictions and gives them unbounded system privileges. This could be abused by the administrator himself, while also raising the risk of successful assumption of the administrator role by unauthorised third parties. Therefore, if possible, different administrative functions should be differentiated. Depending on the administrative role, for example, it is possible for one administrator to only manage printers, another to create new users and a third to be responsible for backups. Ideally, there would even be a separate administrator to analyse logged data and monitor the other administrators' work.

18. Program privileges should be restricted

Executable programs, like users themselves, have certain access rights and system privileges. In many cases a program will simply inherit the permissions of the user who has started it up. Sometimes these authorisations are not sufficient. Or it may be a case of server processes which often have to be configured with extensive privileges. In such cases, programs sometimes possess "root" permissions and can use all the system resources, rather like an "omnipotent" system administrator. If such programs are used by an aggressor in a way in which they were not intended to be used, then the aggressor in turn will inherit all the permissions that go with the misused program. Programs, too, should be configured only with the authorisations that they need to work properly.

19. The standard, factory configured settings need to be modified as appropriate

Many operating systems and software applications are preconfigured by the manufacturer so that, following installation, the product will function in as smooth and convenient a fashion as possible. (The same applies to complete IT systems and private branch exchanges). Unfortunately, IT security aspects often play no role in the choice of standard settings by the manufacturer. Undoubtedly this convenience is fine for users who are not familiar or not adequately familiar with the system concerned. The existing product functionality comes with as few restrictions as possible in the basic configuration and allows unrestricted communication with the environment in which it is used. Often standard passwords and standard user accounts have been configured. To avoid misuse, these must be disabled. A freshly installed system that has not yet been adapted to the actual (security) requirements should therefore never be used in productive operation.

Important servers and operating systems on computers that are particularly exposed need to be toughened or "hardened". In IT security, hardening means removing all those elements of the software

and functions that are not essential to the work that is expected to be carried out with the program. Often an aggressor will succeed in penetrating a server by misusing a program that did not even need to be installed on that server. Moreover, regular maintenance and updating of a computer naturally means more work when it contains more programs. For these reasons, all unnecessary application programs should be removed. The same applies to individual tools, drivers, subcomponents etc. It may even be possible to remove individual "commands" that are not required (i.e. the associated operating system routines).

20. Manuals and product documentation should be read promptly

An experienced administrator will often be in a position to boot up a system without reading the operating manuals in advance. However, this success is often deceptive. Thus, for example, manufacturer warnings can be overlooked, resulting in unexpected problems later on, such as incompatibilities, system crashes or undetected vulnerabilities. It is therefore careless and unprofessional to ignore the help and information provided by the manufacturer and thus create unnecessary risks.

21. Detailed installation and system documentation must be created and updated regularly

It is advisable to document all operator actions performed prior to, during and after an installation in writing. This will make it possible to recover more quickly and also, in case of problems, to locate the possible causes. It is also important that the system documentation can be understood by third parties (e.g. by a "stand-in" administrator or when someone is away on holiday). This reduces the risk of failures in the event that the full-time administrator is suddenly no longer available. Moreover, if a hacker attack is carried out, it will make it possible for unauthorised changes to the system to be identified more quickly.

7.3 Networking and internet connection

For most users with internet access, e-mail and web browsers are the two most important internet applications. It is no wonder that many dangers lurk here. Harmful routines that could escape detection by a virus protection program could sneak in along with files that are downloaded. Unwanted actions can be triggered while surfing on the Internet, especially where risky active content (see safeguard 26) is allowed to execute.

On the BSI's website you will always find up-to-date information, studies on various subjects and also detailed examples under the heading "Internet security".

22. Networks must be protected by a firewall

No computer used for business purposes should be connected to the Internet without the protection of a suitable firewall.

Even within relatively large internal networks there are normally several subnets with different user groups and different protection requirements. Often it is therefore necessary to protect one's "own" subnet against adjacent networks to ward off threats which may be qualitatively similar to threats from the Internet (e.g. isolation of the Human Resources department from the rest of the organisation). Therefore protection mechanisms should be installed on these network connections.

What is a firewall?

A firewall is a hardware or software system that monitors the connection between networks and, in particular, averts attacks on the network (intranet) from the Internet. The possibilities start with simple, sometimes free of charge computer programs ("personal firewalls") that generally only protect the computer on which they are installed. On large networks on the other hand, complex firewall systems that consist of several hardware and software components are used.

23. A secure firewall must satisfy certain minimum requirements

To protect the internal network against neighbouring, less trusted networks, a suitable firewall type must be selected. The design of the firewall architecture and the firewall installation should be left to specialists.

Generally a multi-level firewall concept is recommended, under which additional filter elements (for example routers) are positioned upstream and downstream. In the individual case, if for example there is only a single computer or a complex firewall system is not possible for other reasons, it is recommended installing a personal firewall on the computer to be protected and thus providing at least basic protection.

The filter rules in firewalls tend to grow and become less straightforward with the passage of time. Firewall administrators comply with requests from users all too lightly, thus watering down the rules. There should be no exceptions, not even for the CEO! It is therefore necessary to check at regular intervals whether the existing filter rules are still consistent, whether they can be simplified and whether they are sufficiently restrictive. Moreover, checks should be carried out from time to time as to whether the existing firewall design can still cope from the point of view of IT security with communications protocols that have already been introduced or are expected to enter use before long. Again, new technologies can pose additional challenges to existing firewall concepts. Detailed technical information on firewalls is contained in the IT-Grundschutz Catalogues and on the BSI's website.

Further information on the firewall architecture

Even a firewall can fall victim to a successful attack. Defence strategies that are designed with multiple levels are necessary in order to be able to maintain a minimum amount of protection even where one firewall component has been compromised.

All servers which because of their functionality require direct communication with the Internet and are only separated from the Internet by firewalls or other protection mechanisms (e.g. proxies) should be placed in a demilitarised zone (DMZ). Here the correct cascading and subdivision of servers into different compartments of the DMZ (each with their own range of IP addresses) plays an important role for overall security.

24. Data offered to outsiders should be restricted to the minimum necessary

A lot of sensitive information is provided to authorised users over open networks. This means that confidential data can be accessed from outside. Its protection depends solely on reliable authentication and authorisation mechanisms. If, however, these have been incorrectly configured or contain a vulnerability, then information requiring protection can easily fall into the wrong hands. Such errors tend to be the rule rather than the exception. It is therefore necessary to always check in each individual case whether data requiring protection really does have to be made available and processed outside the organisation's own, well protected network.

25. Services and program functionality offered to outsiders should be restricted to the minimum necessary

Every function, server service or open communication port that is offered to the outside world increases the risk of a possible security loophole. Therefore in every single case it is necessary to check carefully whether it is really necessary to enable and offer a potential "problem candidate" to the outside world. The associated security risk can be quite different, depending on the relevant technology and implementation. With existing installations, regular checks should be carried out as to whether individual services or functions have not simply been enabled by mistake or out of convenience, even though no one needs them. The reduction in administration effort that results from such restrictions means that the time gained can profitably be invested in closer attention to detail in the security administration of the remaining processes.

26. Particular caution should be exercised when handling web browsers; risky actions should be prohibited

Only active content, script languages and multimedia plug-ins that are absolutely essential for work should be enabled in web browsers. Especially risky scripting languages should without exception be disabled.

Additional information

New technical developments mean that the scripts, protocols and add-on programs that one should avoid are continually changing. Up-to-date information on risky technologies is contained on the BSI's website. At present, ActiveX, active scripting and JavaScript are viewed as particularly dangerous.

27. Particular caution should be exercised as regards e-mail attachments

The file attachments appended to incoming e-mails can contain damaging functionality, if executed inadvertently. No user should innocently open such attachments without checking them first. It is imperative to use a virus protection program! In case of doubt, the recipient should check with the originator before opening an attachment. One particular problem is that certain e-mail programs open and execute attachments directly without asking the user for confirmation. Automatic opening of e-mail attachments can be technically prevented by selecting an e-mail program that does not have this functionality, implementing appropriate configuration settings and installing add-on programs.

28. A stand-alone internet PC used for surfing is a low-cost solution for most security problems relating to the use of the Internet

One simple and cheap way of reducing the number of risks associated with surfing on the Internet is to set up a stand-alone PC which is not connected to the internal network. This can be used for internet research without having to forego functionality and convenience. Downloaded files can be checked for viruses on this machine and then be passed on via data media or e-mail into the internal network.

Additional safeguards

It is recommended that security safeguards are technically enforced so as to prevent users from disabling or circumventing security mechanisms either by mistake or intentionally. The transmission of dangerous scripts during surfing or of potentially suspicious e-mail attachments can be prevented through central settings on the firewall and the use of a proxy.

7.4 The human factor: knowledge and heeding of security requirements

29. Security policy and requirements must be followed

A security policy can only help if it is heeded. Even the best security functions and programs are of no avail if they are not used. The consistent observance of all necessary security requirements entails a learning process for every individual and only functions in the long-term once it becomes routine. All staff should have a basic understanding of IT security, be able to follow the line of argument and assess dangers. For even the most sophisticated security policy cannot cover every security aspect of daily working life without exception.

30. Tidiness and order should prevail at the workplace and no sensitive information should be freely accessible

"Orderliness is next to godliness". People may well disagree with this saying, but in the context of IT security, orderliness is without doubt an excellent way of avoiding additional risks. Confidential files should be locked in the cabinet or safe at the end of the day. Data media such as tapes, diskettes and CD-ROMs containing confidential material should never be left lying around. If necessary, they should be properly disposed of to prevent unauthorised persons from reconstructing them. Confidential printouts belong in the shredder and not in the normal waste paper basket. Data media such as hard disks or CD-ROMs must be securely deleted or destroyed.

Of course, implementation of this safeguard depends on data and files having been rated as sensitive in the context of an assessment of protection requirements and staff being familiar with these requirements!

31. Special precautions should be taken in the case of maintenance and repair work

Especially when computers or individual hard disks are repaired or thrown away, it is possible for unauthorised persons to view or reconstruct confidential data (and normally even on defective data media). Service technicians should therefore never work alone unsupervised on IT systems or private branch exchanges. When data media is to be taken off-site, all data must be carefully deleted beforehand.

Caution: Files which are deleted in the conventional way can subsequently be read either wholly or partially using special tools. Important files must therefore be "securely deleted". Add-on programs are available for this purpose for the standard operating systems.

32. Staff must receive regular training

A lot of mistakes arise from ignorance or lack of awareness of potential problems. This statement naturally applies to IT security as well.

Especially for administrators and IT security managers, regular training is essential. However tight budgets may be, it is important not to dispense with training, even if expensive options such as attending outside seminars are not possible. It is always worthwhile purchasing good technical literature.

However, the training should not just cover technical topics. Often, the weakest link in the security chain are the employees. A notorious "expert" revealed in front of US congress how he had managed to get into the networks of well-known large companies to steal information. Only rarely had he resorted to technical attacks. Most of the times it had been easy for him to get the employees to disclose security codes to him.

Safeguards should therefore be taken at regular intervals to increase security awareness among all the staff concerned. This can be done in a variety of ways: internal lectures, training courses, circulated memos, posters, graphic examples, publication of security incidents etc.

It is also important to inform staff of the channels available for communicating with business partners: Who are the contacts? Which competence levels do they have? Which process must be followed for authorisation? Which information may be forwarded to external parties?

Lines of communication, too, need to be explained: What data may be exchanged via e-mail? What are the business partners' correct phone numbers and URLs?

It happens increasingly often that fraudsters direct unsuspecting internet users to manipulated websites (e.g. of banks) via e-mail and ask them to enter sensitive information such as PIN, password or TAN ("phishing").

33. Only an honest self-assessment will help: sometimes it is necessary to call in the experts for advice

The necessary technical knowledge on all aspects of IT security will not always be available within the organisation. Experience suggests that qualification safeguards are often not sufficient as the persons concerned simply do not have time for the technical requirements. Here it is necessary to rethink and redefine responsibilities. In many cases it is more sensible to call on external help or to outsource technical tasks to service providers. Overestimation of one's own capabilities or false economies can have fatal consequences.

34. Audits should be set up for all existing security objectives

Comprehension, acceptance and willingness on the part of staff with regard to all the required security safeguards is always the uppermost aim. However, requirements can be ignored for a number of reasons. Deliberate disregard is the exception rather than the rule. Instead, mistakes and carelessness are the commonest causes. Avoidance through suitable safeguards is in the interests of everyone. For this reason, it is necessary to consider for every security objective how compliance can be monitored. For example, monitoring may entail the use of technical tools, or it can be carried out by auditors, through analysis of logged data, or spot checks by managers etc. Last but not least, the possibility of self-regulation should be offered, for example, by giving suitable checklists for staff to work their way through. Optionally, such completed checklists can then be signed and passed on.

35. The consequences of security breaches should be specified and published

All those involved should be aware that (intentional or unintentional) disregard for security requirements will incur disciplinary safeguards. To underline this, in each case it should be clearly noted (for example, in the organisation's security policy) what consequences may be expected.

36. Detected security breaches should also actually be penalised

If any security breaches are discovered, then the question immediately arises as to how the line manager should deal with the guilty party. Tough sanctions for mild breaches are definitely inappropriate, especially if it is the first such occasion. On the other hand it is equally wrong not to take action in case of more serious breaches or persistent offenders. This would give the wrong signals not only to the guilty person but also to everyone else who finds out about it. Therefore an appropriate response is required where necessary. The fact that breaches will incur disciplinary action must be communicated to everyone else, as far as the situation permits.

7.5 Maintenance of IT systems: handling security-relevant updates

37. Security updates must be regularly installed

In view of the meteoric speed at which new viruses sometimes spread, implementing anti-virus software security updates must be a top priority. Updates of web browsers, e-mail programs and operating systems should likewise be carried out at regular intervals. But other application software and particular hardware components also have to be regularly maintained.

38. Detailed research should be carried out at regular intervals on the security characteristics of the software used

To protect IT systems, it is necessary to keep informed of newly identified vulnerabilities and tools. The latest recommendations on the Internet and technical articles can assist here (e.g. see the "Further information" subsection in the section on CERTs). In "more recent" program versions (e.g. of browsers), security-relevant vulnerabilities have usually been eliminated by the manufacturer. However, this does not obviate the need to consider the matter on an individual basis, as new versions usually contain new functions and bugs that bring other dangers.

Every system manager should regularly set aside time for appropriate searching on the Internet and to exchange information with professional colleagues. As before, there are plenty of information services available that are free of charge and which often are superior to those of commercial suppliers.

Moreover, the abundance of updates and security patches that are constantly being published makes a selection process necessary. Usually they cannot all be installed, especially as an immediate safeguard. Therefore there should be agreement in advance on the selection criteria to be applied when deciding which updates can or must be installed and with what time delay.

39. An action plan for installing any necessary security updates should be created

Even if the system manager does not install important security updates, this does not mean either that the system automatically stands still or that a malicious hacker attack will take place immediately. This makes clear that the installation of updates requires a lot of discipline and must be laid down in advance as a process. In the case of anti-virus software, the fastest possible installation of updates should become the routine.

40. Software changes should be tested

In theory, every software change to productive systems should be exhaustively checked in advance in a test environment to ensure that all the systems will still function smoothly once the change is

implemented. There have even been instances where a virus protection program update paralysed a corporate network as in-house software was incorrectly identified by it as a new virus and disabled.

Testing of important security updates usually takes place under particular time pressure, as they need to be installed as soon as possible. In practice, administrators must therefore weigh up carefully the IT security requirements and the available resources and make reasonable compromises.

7.6 Use of security mechanisms: handling passwords and encryption

41. Security mechanisms should be selected carefully

Many manufacturers have already integrated optional security mechanisms such as password protection or encryption into their products. The design of secure encryption mechanisms is an extremely demanding science. Product developers who have not devoted several years to the subject could therefore never develop secure procedures. But there are also a lot of product manufacturers whose products offer self-developed encryption mechanisms, which usually are not secure. If one is reliant on secure procedures, one should enquire critically what procedures the manufacturer employs. If possible, these should be standard, generally recognised algorithms.

Even if doubts exist as to the quality of a particular security function, it is recommended using it if there is no more effective alternative: poor protection is better than no protection. However, the existing protection mechanisms should then be operated at the maximum protection level. In practice, many suppliers of online services that use SSL encryption, for example, still allow key length of 40 bits in order to maintain compatibility with older web browsers.

42. Passwords should be well chosen (secure)

Poor passwords are among the top items on a hit list of IT security shortcomings that occur most frequently. In particular, hackers can exploit poorly chosen passwords. To protect oneself against hackers' tools which automatically try out every conceivable character string combination or entire dictionaries, including commonly used combinations of words and added numbers, a password must satisfy certain quality requirements. Passwords should be over seven characters long, should not be dictionary words, nor should they consist of names (especially not favourite heroes from literature and cinema), and they must also contain special characters or numerals. In the latter case, commonly found variants, such as attaching a single digit to the end of the password or adding one of the main special characters \$, !, ? or # at the beginning or end of an otherwise simple password, should be avoided.

The sensible requirement that every password should be changed at regular intervals creates a dilemma, in that it is difficult to remember a lot of passwords. Apart from a few exceptions in high security areas, it is therefore legitimate to write one's passwords down and keep them in a secure location (but naturally not on the screen or in the top desk drawer).

The habit of using a single password for many different purposes or accounts is also problematic. If the password for one application falls into the wrong hands, then a clever attacker will also try that password out in other applications belonging to the same person. The advantages and disadvantages of such "aids to convenience" should therefore be weighed up from case to case.

43. Predefined or blank passwords should be changed

Many software products are supplied with accounts whose password is blank or always the same and generally known. A lot of hackers know this, and during an attempted attack first of all they check to see whether the need to give these accounts new passwords has been overlooked. Hence, where products are freshly installed, one should always refer to the manual to see whether any such accounts exist. Maintenance companies which use poor or fixed passwords for external maintenance access are another security problem. In individual cases it is known that manufacturers have installed undocumented "backdoors" in their programs, for example, so as to obtain administrative access easily in case of support. Manufacturers or maintenance companies should therefore be able to explicitly provide assurance that they have not employed such methods.

This warning refers not only to IT systems but also to modern private branch exchanges.

44. Workstations should be secured in the absence of their owner by a password-protected screensaver

Every common operating system offers the possibility of locking the keyboard and screen after a certain idle time. To unlock them it is then necessary to enter the correct password. Screensavers should be used if unauthorised third parties could gain access to a PC during the temporary absence of its rightful owner. The lock should not be activated too quickly, otherwise it disturbs the user after short pauses in user inputs. A frequently used interval is five minutes after the last user input. It should also be possible, if required, to immediately activate the lock. Under Windows this is available after pressing <Ctrl+Alt+Del>.

45. Sensitive data and systems must be protected

By the time that someone obtains direct access to a hard disk containing sensitive data, unencrypted data is generally freely readable. The protection mechanisms built in to the operating system or the relevant application offer only inadequate protection against access by experts. The use of encryption software for confidential files should therefore be considered. If possible, notebooks should be entirely encrypted because they can be stolen quite easily. Good products are available quite cheaply or even free of charge. When selecting a product, care must be taken to ensure that the protection mechanisms used are secure. Algorithms developed in-house by manufactures are seldom secure. Information on secure algorithms and key lengths can be obtained from technical books, from the BSI or on specialist security sites on the Internet.

7.7 Protection against catastrophes and damage by the elements

46. Emergency checklists should be created and every employee should be familiar with them

Every employee should know what to do if a computer fails, the printer will not print any more, there is a power failure, the network is infected by a virus or data is accidentally deleted. All those responsible should act out the conceivable scenarios and note down the names of responsible persons and their phone numbers in a list. A brief description of typical scenarios is also useful. Examples: how is a backup restored? How is the printer server restarted?

47. All important data must be backed up regularly

A large variety of software and hardware data backup solutions are available. It is important that all relevant data is actually captured by the configured backup. This may be quite a challenge in the case of distributed heterogeneous environments. Mobile terminal devices such as notebooks, non-networked stand-alone computers and PDAs must be included. It is necessary to verify at regular intervals that the backup procedure does in fact work and the data can be successfully restored.

The backup media must be kept in a safe place, if possible outside the company or office building. The storage location also needs to be adequately protected against damage by the elements, e.g. fire, water and similar.

All users must know what data is backed up, when it is backed up and for how long it is stored. Normally only certain directories and files are backed up; a complete backup is seldom carried out.

48. IT systems must be appropriately protected against fire, overheating, damage due to water and power failure

It is not just through user error or malicious attacks that IT assets can sustain damage. Often serious damage results from the physical effects of fire, water or power. A lot of equipment can only be operated under certain climatic conditions. Therefore, IT components that are particularly important (servers, backup media, routers etc.) should be stored in adequately protected rooms. In addition, they should be connected to an uninterruptible power supply with overvoltage protection. Useful tips on implementation can be obtained from the public fire service and also from the BSI (see also the information contained in the IT-Grundschrift Catalogues on this subject).

49. Access protection safeguards and safeguards to protect against break-in must be implemented

Even small companies and agencies should think about protecting themselves against intruders and other unwanted visitors. Some simple safeguards can significantly improve security. One should think about where visitors and outsiders generally go and what IT systems they could access from there.

Especially servers or computers that are used to access sensitive data should be configured in such a way that outsiders cannot interfere with them unobserved. Visitors should be attentively looked after, not just out of politeness. It may be appropriate to close certain offices during staff absences or not to leave windows ajar (e.g. during the lunch break). Activities by tradesmen, service technicians and cleaning staff should be deliberately planned and notified to all staff. Notebooks should never be left unattended in cars and, if appropriate, should be locked in the office overnight or during longer absences. The guidance given here is not complete – it needs to be reviewed and supplemented on a case-by-case basis.

Tip:

Have your anti-intrusion safeguards checked by experts or police advisers so you can avoid making it unnecessarily easy for intruders.

50. All hardware and software should be recorded in an inventory list

An inventory list that is updated regularly is recommended. In many cases this information can be taken from the accounting data. But even then there is often uncertainty about the last location or whether a missing object was already missing at a certain point in time or has only gone missing recently. Insurance companies also require inventory lists with valuations so that insurance claims can be dealt with in an ordered fashion. The inventory list is also useful for checking regularly that the sum insured is adequate.

8 The BSI's IT-Grundschrift methodology

Earlier chapters have examined various aspects of IT security and explained why an adequate level of security cannot be achieved by technical mechanisms and functions alone. On the contrary, the technical security functions must be accompanied by safeguards covering organisational, staff-related and physical building aspects. Anyone seeking to systematically and comprehensively improve IT security faces the challenge of how to achieve the best possible security functionality at a reasonable cost. In addition, the implemented solutions must be practicable and sufficiently convenient that they are also accepted by those concerned in their daily work. This chapter describes procedures to follow when drawing up professional IT security concepts and explains how the BSI's IT-Grundschrift methodology can help you with this.

8.1 The BSI's IT-Grundschrift methodology as the basis for a professional IT security concept

Comprehensive but expensive: the risk assessment

One way of creating a security concept is the traditional risk assessment. This entails devising individual security safeguards for an existing IT environment. The assets to be protected (IT systems, data, know-how etc.) are ascertained and examined to see which threats they are exposed to. The next stage is to analyse the probability of a security incident, the likely extent of damage, what security safeguards can be taken and what residual risks will remain after the security concept has been implemented.

Risk assessments provide valuable information, but are associated with a lot of work because of the need to carry them out on an individual basis: experts with appropriate know-how are needed. The relevant input variables, such as the probability or extent of damage, are very difficult to ascertain and at best can only be calculated roughly. A risk assessment is therefore associated with high costs.

The BSI's IT-Grundschrift methodology as an efficient alternative

The BSI's IT-Grundschrift methodology constitutes an alternative means towards creating a security concept. The IT-Grundschrift methodology is based on the BSI standard 100-2 describing the IT-Grundschrift approach and the IT-Grundschrift Catalogues containing the module, threat and safeguard catalogues. IT-Grundschrift builds on the fact that the majority of the IT systems and applications used in practice are run in a similar fashion and in comparable operational environments. Servers under UNIX, client PCs under Windows and database applications are examples here. Through the use of these typical components, the same kinds of threats to IT operations are found on a recurring basis. If there are no special security requirements, these threats are largely independent of the specific application scenario. This leads to two ideas for proceeding:

- ▶ An all-embracing risk assessment is not always necessary: the threats to IT operations and the probability of damage resulting from these threats can be roughly calculated if certain assumptions are made.
- ▶ It is not always necessary to develop new security safeguards for every application: groups of standard security safeguards can be derived which offer an appropriate and adequate degree of protection against these dangers under normal security requirements.

On the basis of these assumptions, the IT-Grundschrift approach suggests a methodology for creating and checking IT security concepts. The BSI standard 100-2 on the IT-Grundschrift approach explains step-by-step how an IT security management system can be developed and operated in practice. The IT-Grundschrift approach explains in extensive detail how an IT security concept is drawn up in practice and how appropriate IT security safeguards can be identified and implemented. IT-Grundschrift therefore interprets the very general requirements of the above-mentioned ISO 13335, 27001 and 27002 standards and provides users with practical help in the form of numerous tips, background knowledge and examples. One of the most important objectives of IT-Grundschrift is to

reduce the expense of the IT security process by offering bundles of familiar, reusable procedures to improve information security. Thus, the IT-Grundschutz Catalogues contain standard risks and security safeguards for typical IT systems that can be used in one's own organisation as required. They describe field-proven standard security safeguards for typical IT systems that are to be implemented incorporating the latest technology, with a view to achieving a reasonable level of security. In doing so, the manual considers the areas of infrastructure, organisation, personnel, technology and contingency planning and thus supports an integrated approach. Particular emphasis is placed on obtaining the necessary technical knowledge. This makes the IT-Grundschutz Catalogues suitable for use as a reference work as well.

IT-Grundschutz users enjoy advantages

Using the IT-Grundschutz approach, it is possible to implement IT security concepts simply and economically in terms of the resources required. The attainable level of security is adequate and reasonable for normal protection requirements and can serve as the basis for IT systems and applications which require a high level of protection. Only if the protection requirement is significantly higher or the IT systems concerned are not covered in the IT-Grundschutz Catalogues is it necessary to carry out a supplementary security analysis. All in all, **orienting oneself to the IT-Grundschutz approach** brings the following benefits:

- ▶ Standard security safeguards are described in concrete detail.
- ▶ The resulting IT security concepts are scalable, can be updated and are compact, as they refer to an existing reference source.
- ▶ The security safeguards to be implemented are field-proven and have been selected so that their implementation will be as inexpensive as possible.
- ▶ Even if someone should not wish to create a complete security concept, thanks to the modular structure the IT-Grundschutz Catalogues can serve as technical guidelines and a source of advice on a wide range of security issues, which obviously is beneficial.

In Germany, IT-Grundschutz has established itself as a virtual standard and is recommended by various institutions, such as the Federal Commissioner for Data Protection, as a method for creating security concepts.

The IT-Grundschutz tool



In addition to the documentation on IT-Grundschutz, the BSI provides special software in the form of the BSI IT-Grundschutz Tool (GSTOOL). It supports users in the creation, administration and updating of IT security concepts based on IT-Grundschutz. Once the necessary information has been captured, the user has a comprehensive reporting system that allows structured evaluations of all the collected data. A fully functional test version can be obtained free of charge. Further information on GSTOOL can be obtained at www.bsi.bund.de/gstool.

Publication sources

The IT-Grundschutz Catalogues are regularly updated by the BSI. The IT-Grundschutz methodology as well as the IT-Grundschutz Catalogues



are available free of charge in both German and English on the Internet. In addition, they can be obtained along with other BSI recommendations in various electronic versions (HTML, PDF and DOC) as a CD-ROM. The printed version is published by the Bundesanzeiger-Verlag and can be obtained through bookstores.

All publications covering every aspect of IT-Grundschutz and the IT-Grundschutz Certificate, which is based on this, are basically offered free of charge to anyone interested. As long as the content is not altered or used commercially, they can also be disseminated over a company's intranet.

The staff of the BSI can be contacted by members of the public, companies and public agencies regarding questions and suggestions by e-mail (gshb@bsi.bund.de). There is also a telephone hotline (+49 (0)3018 9582-5369).

All information regarding IT-Grundschutz is available on the Internet at

- ▶ www.bsi.bund.de/gshb or
- ▶ www.it-grundschutz.de

8.2 Structure of the IT-Grundschutz Catalogues

The various modules of the IT-Grundschutz Catalogues are structured in accordance with their particular focus into five areas:

1. Organisation-wide IT security aspects

This contains modules on personnel, IT security management and data backup concept.

2. Architectural and structural factors

This group contains modules on buildings, server rooms and home office.

3. IT systems

The IT-Grundschutz Catalogues provide individual modules for typical IT systems such as UNIX systems, laptop PCs and private branch exchanges.

4. Networking aspects of IT systems

Networking aspects such as heterogeneous networks or network and system management are covered here.

5. IT applications

Specific modules are provided for applications such as e-mail, web servers and databases.

Every module of the IT-Grundschutz Catalogues contains a brief description of the subject and a list containing references to the relevant threats in question and to the relevant standard security safeguards.

8.3 Performing an IT-Grundschatz analysis

The IT-Grundschatz approach (BSI standard 100-2) describes a methodology for creating or checking IT security concepts on the basis of standard security safeguards for IT solutions. Extensive information is also provided on how to implement security safeguards and maintain IT security during ongoing operations. The standard security safeguards described in the IT-Grundschatz Catalogues constitute a basic level of security that is reasonable and adequate for normal security requirements. However, even where the protection requirement is higher, the IT-Grundschatz Catalogues contain useful recommendations. It may be necessary for these to be supplemented by additional, more extensive IT security safeguards. Supplementary security safeguards could, for example, also be necessary where special components that are not covered in the IT-Grundschatz Catalogues are used but which play an important role for the overall security of the IT assets.

The main steps in the IT-Grundschatz methodology are as follows:

6. IT structure analysis

This entails gathering information about the information technology assets in the area under consideration. It is important to document applications, IT systems and IT rooms and demonstrate dependencies. Here one should limit oneself to the most important components and present the results clearly.

7. Assessment of protection requirements

The aim of the assessment of protection requirements is to ascertain how much effort needs to go into protecting IT applications, IT systems, communications connections and rooms against impairment of confidentiality, integrity and availability. Only in this way is it possible to achieve an adequate level of protection at the lowest possible cost.

8. Modelling

Modelling is a central step in the application of the IT-Grundschatz methodology. During modelling, the modules in the IT-Grundschatz Catalogues are assigned to the existing processes and components ("target objects"). The IT-Grundschatz Catalogues contain a precise description of how a real set of IT assets can be modelled as accurately as possible using the existing modules.

Thus, for example, the chapter "IT Security Management" is applied once to the entire set of IT assets, while the "Fax Machine" module is applied to each individual fax machine. Every chapter contains a description of the relevant threats and IT security safeguards for the corresponding target object. The outcome of the modelling process is an extensive list with IT security safeguards.

Using this catalogue of safeguards, it is possible in the next step to check which IT security safeguards have already been implemented in practice or where vulnerabilities still exist (target versus actual comparison). When planning a set of IT assets, the catalogue of safeguards can serve as the basis for a specification.

9. Basic security check

If the IT-Grundschatz methodology is applied to an existing set of IT assets, it is necessary to check which of the standard security safeguards that have been identified as necessary in the modelling process have already been implemented and where shortcomings still exist. To this end, interviews are carried out with those responsible and spot checks are performed. This operation is referred to as the basic security check.

9 Standards and certification of one's own IT security

If an organisation wishes to be able to demonstrate that it satisfies defined security standards, certification is recommended. The summary below provides descriptions of the orientation of each individual procedure. Well-known standards for which official certification is not possible are also mentioned here as misunderstandings on this frequently occur.

Certification in accordance with Common Criteria (ISO/IEC 15408)

Common Criteria (CC) is an internationally recognised standard for the certification of hardware and software products. The aim is to prove that the security requirements of an IT product or IT system have been implemented in full and correctly and, in particular, that the security functions cannot be circumvented due to vulnerabilities. The complexity of testing and the resulting degree of trust in the effectiveness of the security performance of the certified product depend on the depth of testing. The CC standard identifies seven evaluation assurance levels (EAL 1 to 7), which are oriented to the assumed perpetrator profile, the motivation of the perpetrator, his expertise and the amount of time and equipment needed to carry out an attack.

Cobit

Cobit (Control Objectives for Information and related Technology) describes a method for monitoring risks resulting from the use of IT to support business-relevant processes.

The Cobit documents are published by the "IT Governance Institute" (ITGI) of the "Information Systems Audit and Control Association" (ISACA). When they developed Cobit, the authors oriented themselves to existing standards on the subject of IT security management, such as the NIST Security Handbook and ISO 27002 (previously ISO 17799).

Cobit certification is strictly speaking not possible. Many auditors use the criteria to check the IT control environment in the context of the annual audit.

ITIL

The IT Infrastructure Library (ITIL) is a collection of books on the subject of IT service management. It was developed by the United Kingdom's Office Of Government Commerce (OGC) in accordance with ISO 9001, with the collaboration of a number of companies and external experts.

ITIL is concerned with the management of IT services from the point of view of the IT service provider. The IT service provider can be both an internal IT department or an external service provider. The overriding objective is to optimise or improve the quality of IT services and cost-effectiveness.

The ITIL approach is entirely process-based and is oriented towards "best practices".

ISO 13335 (GMITS)

The ISO/IEC 13335 standard (Management of Information and Communications Technology Security) (formerly "Guidelines on the Management of IT Security") serves as a general guideline for the initiation and implementation of the IT security management process. It provides instructions but not solutions for managing IT security. The standard is a fundamental work in this area and is the starting or reference point for a whole series of documents on IT security management. There is no provision for certification in accordance with this standard.

ISO 27001

Due to the complexity of information technology and the demand for certification, numerous manuals, standards and national norms for IT security have emerged over the past several years. The ISO 27001 standard "Information Technology – Security Techniques – Information Security Management Systems Requirements Specification" is the first international standard for IT security management that also allows certification. ISO 27001 provides general recommendations on around ten pages. The

controls from ISO/IEC 27002 are referred to in a normative annex. However, the reader is not provided with any assistance for practical implementation.

ISO 27002 (formerly ISO 17799)

The aim of ISO/IEC ISO 27002 "Information Technology – Code of Practice for Information Security Management" is to define a framework for IT security management. ISO 27002 is therefore primarily concerned with the steps necessary for developing a fully-functioning IT security management and for integrating this securely in the organisation. The necessary IT security safeguards are touched on briefly on the approx. 100 pages of the ISO/IEC 27002 standard. The recommendations relate to the management level and contain almost no specific technical information. Their implementation is one of the many options available for fulfilling the requirements of the ISO 27001 standard.

Certification in accordance with ISO 27001 on the basis of IT-Grundschutz

Since January 2006, the German Federal Office for Information Security (BSI) offers certification in accordance with ISO 27001 on the basis of IT-Grundschutz. This certification can be used to demonstrate that the essential requirements of ISO 27001 have been implemented in a set of IT assets by applying the IT-Grundschutz methodology (BSI standard 100-2) and a supplementing risk analysis (BSI standard 100-3), if required. In addition, the BSI offers two preliminary stages for this certificate which serve as a migration path towards actual certification: the "Auditor's Attestation Entry Level" and the "Auditor's Attestation Advanced Level". The individual levels differ with respect to the number of safeguards to be implemented. Each safeguard included in an IT-Grundschutz module is assigned to one of these three levels so it can be easily seen which concrete security recommendations from the IT-Grundschutz Catalogues have to be implemented.

An application for an Auditor's Attestation can be lodged by an organisation with the BSI after all the safeguards that are relevant to that level have been implemented and an *internal* audit has been carried out as to whether the implementation follows the test scheme. An Auditor's Attestation is valid for two years and cannot be extended as it is designed as a preliminary stage to certification.

Once all the safeguards that are relevant for certification have been implemented, the organisation can commission a licensed auditor to test the IT assets against the BSI's test scheme. The results of this independent test are documented in an audit report. ISO 27001 certification on the basis of IT-Grundschutz can be applied for on submission of the audit report to the BSI. The certification office issues the certificate following a check of the report by BSI experts and the certificate and the auditor's attestation are published by the BSI. All information related to the certification such as the certification method and the names of the licensed auditors are publicly available, including on the Internet at www.bsi.bund.de/gshb/zert.

10 Annex

10.1 Checklists

The questions contained in this chapter summarize the content of the 50 IT security safeguards outlined above and provide a quick overview of the vulnerabilities in one's own organisation.

IT security management	
<input type="checkbox"/>	Has management defined the IT security objectives and accepted that they are responsible for IT security? Have all the legal and contractual issues been considered?
<input type="checkbox"/>	Is there an IT Security Officer?
<input type="checkbox"/>	Are IT security requirements considered early on in every project (e.g. during planning of a new network, new purchases of IT systems and applications, outsourcing and service agreements)?
<input type="checkbox"/>	Is there a summary of the most important applications and IT systems and their protection requirements?
<input type="checkbox"/>	Is there an action plan that prioritises security objectives and defines how the agreed IT security safeguards should be implemented?
<input type="checkbox"/>	Has it been determined for all IT security safeguards whether they have to be carried out once only or at regular intervals (e.g. updates to the anti-virus software)?
<input type="checkbox"/>	Have responsibilities been defined for all the IT security safeguards?
<input type="checkbox"/>	Are appropriate deputisation arrangements in place for persons in positions of responsibility and are the stand-ins familiar with the tasks they have to perform in this capacity? Have the most important passwords been securely deposited for emergencies?
<input type="checkbox"/>	Are all involved persons familiar with the existing policies and responsibilities?
<input type="checkbox"/>	Are there checklists covering factors that need to be considered when new staff join or existing staff leave the company (authorisations, keys, training etc.)?
<input type="checkbox"/>	Is the effectiveness of IT security safeguards checked regularly?
<input type="checkbox"/>	Is there a documented IT security concept?

Security of IT systems	
<input type="checkbox"/>	Are protection mechanisms in applications and programs used?
<input type="checkbox"/>	Is anti-virus software used across the board?
<input type="checkbox"/>	Have roles and profiles been assigned to all system users?
<input type="checkbox"/>	Are controls in place as to which data each member of staff is allowed to access? Are there sensible restrictions?
<input type="checkbox"/>	Are there different roles and profiles for administrators, or is every administrator allowed to do everything?
<input type="checkbox"/>	Are the privileges and permissions of programs known and controlled?
<input type="checkbox"/>	Are security-relevant standard settings of programs and IT systems suitably adapted or is the delivery state retained?
<input type="checkbox"/>	Are unnecessary security-relevant programs and functions systematically uninstalled or disabled?
<input type="checkbox"/>	Are manuals and product documentation read promptly?
<input type="checkbox"/>	Is detailed installation and system documentation created and updated regularly?

Networking and internet connection	
<input type="checkbox"/>	Is there a firewall?
<input type="checkbox"/>	Are the configuration and functionality of the firewall monitored and critically examined at regular intervals?
<input type="checkbox"/>	Is there a concept as to which data has to be offered to the outside world?
<input type="checkbox"/>	Has it been specified how dangerous add-on programs (plug-ins) and active content should be avoided?
<input type="checkbox"/>	Have all unnecessary services and program functions been disabled?
<input type="checkbox"/>	Are web browsers and e-mail programs securely configured?
<input type="checkbox"/>	Have all staff been adequately trained?

Compliance with security requirements	
<input type="checkbox"/>	Are confidential information and data media stored carefully?
<input type="checkbox"/>	Is confidential information deleted from data media or IT systems prior to maintenance and repair work?
<input type="checkbox"/>	Do staff receive regular training on security-relevant subjects?
<input type="checkbox"/>	Are there safeguards in place that are aimed at increasing the security awareness of the workforce?
<input type="checkbox"/>	Are existing security regulations monitored and security breaches disciplined?

Maintenance of IT systems: handling updates	
<input type="checkbox"/>	Are security updates regularly installed?
<input type="checkbox"/>	Has someone been appointed to keep up-to-date on security characteristics of the software used and relevant security updates?
<input type="checkbox"/>	Is there a test concept for software modifications?

Passwords and encryption	
<input type="checkbox"/>	Do programs and applications provide security mechanisms such as password protection and encryption? Have the security mechanisms been activated?
<input type="checkbox"/>	Have default or blank passwords been changed?
<input type="checkbox"/>	Are all staff trained in choosing secure passwords?
<input type="checkbox"/>	Are workstations protected in the absence of their owner by a password-protected screensaver?
<input type="checkbox"/>	Are confidential data and systems that are especially at risk such as notebooks adequately protected using encryption or other safeguards?

Contingency planning	
<input type="checkbox"/>	Is there a contingency plan with instructions and contact addresses?
<input type="checkbox"/>	Are all necessary contingency situations covered?
<input type="checkbox"/>	Is every member of staff familiar with the contingency plan and is this easy to access?

Data backups	
<input type="checkbox"/>	Is there a backup strategy?
<input type="checkbox"/>	Have rules been laid down as to what data should be backed up and for how long?
<input type="checkbox"/>	Do backups also include laptop computers and non-networked systems?
<input type="checkbox"/>	Are the backup tapes checked regularly?
<input type="checkbox"/>	Are the backup and restore procedures documented?

Infrastructure security	
<input type="checkbox"/>	Are the IT systems adequately protected against fire, overheating, damage due to water, overvoltage and power failure?
<input type="checkbox"/>	Is access to important IT systems and rooms controlled? Do visitors, tradesmen, service staff etc. have to be accompanied and supervised?
<input type="checkbox"/>	Is there adequate protection against intruders?
<input type="checkbox"/>	Is all hardware and software recorded in an inventory list?

10.2 Example: What should be regulated in the security concept for a private branch exchange

- ▶ A PBX manager and deputy should be appointed.
- ▶ Any unnecessary features should be identified and disabled.
- ▶ Any factory-configured passwords should be amended.
- ▶ Passwords which are required for configuration and maintenance should be deposited in a secure location for emergencies.
- ▶ Guidelines on premium-rate service numbers and international calls should be issued (e.g. blocking of 0190 and 0900 call numbers).
- ▶ Log files should be analysed regularly so that anything unusual is spotted. This includes, for example, unauthorised dialling in via maintenance lines, calls made after work, repeated calls to systematically try out different PINs, activation of room monitoring equipment etc.
- ▶ The configuration of the PBX should be backed up regularly.
- ▶ Technical documentation and a brief set of instructions for daily use should be created or obtained from the manufacturer.
- ▶ The PBX should be listed in the Emergency Procedure Manual (e.g. containing troubleshooting possibilities, telephone number of a service technician etc.).
- ▶ Staff should be informed about threats (e.g. about the possibility of misusing the room surveillance function on mobile phones, fixed network devices and answering machines to overhear confidential meetings).
- ▶ If possible, the security of the PBX should be checked regularly by external experts.

10.3 Additional information

There is a vast amount of information freely available on the Internet from quite different and often very good information sources on IT security issues. Use a search engine to gain your own impression! You will find that you do not need to reinvent the wheel, but that many documents already exist which offer a good basis for one's own purposes. Some interesting addresses providing further information on the certification and standards mentioned in this document are given below.

General information on IT security

- ▶ **www.bsi.bund.de**
The **Federal Office for Information Security (BSI)** website provides up-to-date information and advice on IT security issues, technical analyses and studies which can be downloaded free of charge. You will also find information there on how to order the CD version of the IT-Grundschrift material and numerous useful links to interesting internet sites.
- ▶ **www.bsi-fuer-buerger.de**
For newcomers to the subject of IT security, the BSI offers a separate information page. Without going into technical details, this explains the most important basic facts on every aspect of IT security in an entertaining way.
- ▶ **www.mittelstand-sicher-im-internet.de**
The German Federal Ministry of Economics and Labour operates this website to provide SMEs with information on a variety of issues related to IT security.
- ▶ **www.a-sit.at**
The Centre for Secure Information Technology - Austria (A-SIT) in Austria was founded as a non-profit alliance between the Federal Ministry of Finance, the Austrian National Bank and the Technical University of Graz. Its website contains a lot of interesting information on many IT security issues, including the Austrian IT Security Manual (ITSHB).
- ▶ **www.isb.admin.ch**
In Switzerland the "Informatikstrategieorgan Bund" (ISB) is concerned with IT security and supports the federal administration. A lot of interesting catalogues of safeguards and guidelines (in German) are freely available.
- ▶ **www.bitkom.org**
The German Association for Information Technology, Telecommunications and New Media (BITKOM) has published various documents (in German) on IT-security issues such as e-mail and internet usage in enterprises, security of company-wide IT-systems and networks, IT security standards and liability risks.
- ▶ **www.bankenverband.de/**
The Association of German Banks regularly publishes information on secure online banking (see, for example, their "Brochures" section).

Information on the BSI's IT-Grundschrift methodology

- ▶ **www.bsi.bund.de/gshb**
Here you will find full details regarding the IT-Grundschrift approach, the IT-Grundschrift Catalogues, GSTOOL and ISO 27001 certification on the basis of IT-Grundschrift.

German CERTs (Computer Emergency Response Teams)

Information on computer viruses and security problems in software and hardware that have been newly identified is published on the information pages of Computer Emergency Response Teams (CERTs). CERTs answer questions related to IT security issues, publish up-to-date information on vulnerabilities and provide information on incidents related to IT security. Based on this information, the system administrators or end users in charge can immediately take concrete steps to avert threats. This way, possible damage is already avoided in advance.

If a security incident occurs, some CERTs offer reactive services to mitigate the consequences, to remedy the damages, or to resolve the incident.

- ▶ **www.bsi.bund.de/certbund**
The BSI operates a CERT for the German Federal authorities (the CERT-Bund) and offers, e.g., an up-to-date e-mail newsletter on various security issues as part of its warning and information service WID (Warn- und Informationsdienst). The CERT-Bund services are primarily provided for the main target group in the German Federal administration.
- ▶ **www.buerger-cert.de**
Here, CERT-Bund and Mcert operate a joint platform which is primarily intended for regularly informing citizens about current security and virus warnings. Apart from getting information on the latest security and virus warnings, users also have the possibility to subscribe to the BSI's newsletter "Sicher • Informiert" which explains current issues in brief. The service provided here is completely free of charge.
- ▶ **www.CERT-Verbund.de**
The CERT-Verbund is an alliance of German CERTs who have committed themselves to cooperate on the basis of a Code of Conduct. This alliance is open to all interested German CERTs.
- ▶ **www.cert.dfn.de**
The German research network (Deutsches Forschungsnetz, DFN) traditionally operates the CERT for the German Research and Education Community. They offer mailing lists for all interested persons.
- ▶ **www.mcert.de**
Mcert is specifically oriented towards small and medium-sized enterprises. Among others, the German Association for Information Technology, Telecommunications and New Media (BITKOM), the German government and private companies participate in this CERT.
- ▶ **www.cert.org**
This is an English-language site of a well-respected CERT that has been in operation for many years and was also the first of its kind.

Standards and certification

- ▶ **www.initiatived21.de/druck/news/publikationen2002/doc/22_1053502380.pdf**
The D21 initiative has brought together and compared the most important IT security standards in an article.
- ▶ **www.isaca.org**
Cobit can be reached on the site of the "Information Systems Audit and Control Association & Foundation".
- ▶ **www.iso.org**
ISO standards can be purchased on the ISO website. Unfortunately they are normally not cheap.
- ▶ **www.commoncriteria.org**
The Common Criteria standard mentioned above can be downloaded free of charge from the

respective homepage. Anyone seeking further details on this subject will also find a wealth of additional information there.

- ▶ **www.isfsecuritystandard.com**
Several large companies have joined forces in the Information Security Forum (ISF) to jointly work on IT security issues. A very good set of guidelines on information security, "The Forum's Standard of Good Practice", is available to the public (in English).

Data protection and the law

- ▶ **www.bfdi.bund.de**
The Federal Commissioner for Data Protection and Freedom of Information provides valuable information on every aspect of data protection on his website. This includes the addresses and links to the State Data Protection Officers who also offer extensive information on the subject of IT security.
- ▶ **www.datenschutz.de**
The "Virtual Privacy Office" is a project involving, amongst others, the Privacy Commissioners both at national and state level. It is above all intended to serve as a single portal to the (primarily German language) data protection knowledge on the Internet and contains a large number of contributions and articles.
- ▶ **www.heise.de/ct/03/07/192/default.shtml**
Here you can find an article from the German computer magazine *ct* including a commented list of some important sources of legal literature.

Date: June 2007