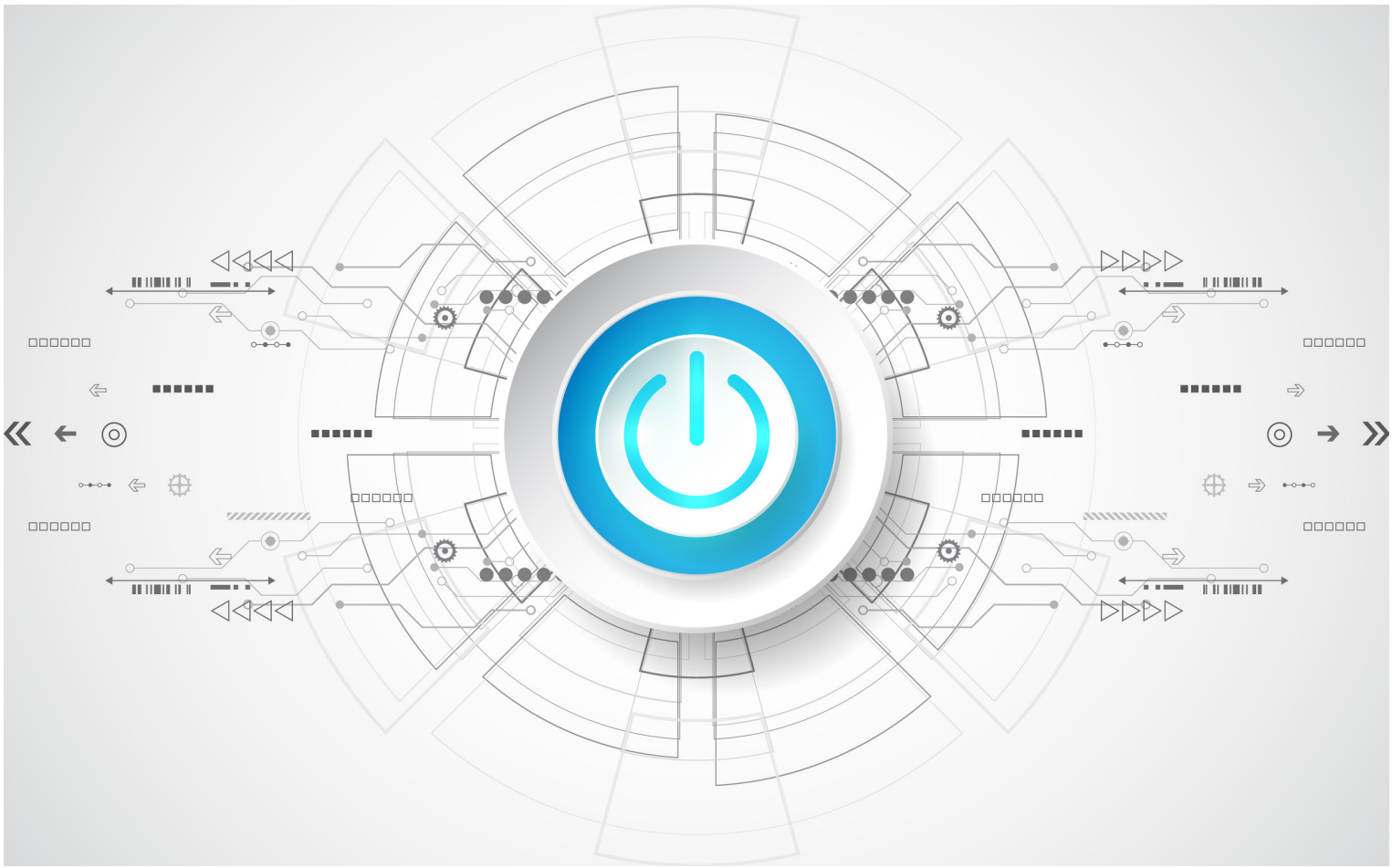
Bundesamt
für Sicherheit in der
Informationstechnik

Guide to Basic Protection based on IT-Grundschutz

3 Steps to Information Security



www.bsi.bund.de/grundschutz

Section IT-Grundschutz
<grundschutz@bsi.bund.de>

Picture credits title photo: kran 77, Fotolia

Foreword

Cyber security is a wide, abstract term. However, filling it with life starts in the smallest organisation. Not only the government can contribute to cyber security in Germany, but also every company – regardless of the size – must make a contribution. With the IT-Grundschutz, the BSI has been providing a proven method and an extensive offer for many years which is successfully used in the administrative and industry sectors. Many government agencies and large companies are – also due to their financial and personnel resources – well positioned when it comes to information security.

However, the exchange with small and medium-sized enterprises mostly – still – reveals a different picture. Even though the awareness for information security issues is given, there is often a lack of trained personnel and financial resources for a sustained and reasonable implementation of the necessary safeguards.

As the national cyber security authority, it is our claim to design the information security in the digitalization and to increase Germany's resistance against cyber threats. The design also involves to offer feasible and target-oriented solutions. This is exactly where this guide to "Basic Protection" starts: As part of the complete IT-Grundschutz Methodology, Basic Protection provides an entry point for all companies who would like to look into the safeguarding of their IT systems and data for the first time. The guide explains in a comprehensible manner the steps required for reviewing the existing information security level as well as safeguards that can be quickly implemented with minimum financial investment and a small number of employees. In addition to technical aspects, infrastructural, organisational and personnel issues will be considered in line with a holistic management system for information security.

I hope you find this a stimulating read that adequately addresses your questions about information security, and most of all that it leads you to a successful implementation of the safeguards described.

Yours faithfully,

Arne Schönbohm

President of the Federal Office for Information Security

Table of contents

1 Introduction

The challenges for authorities and companies to protect sensitive data and communication processes from unauthorised access are constantly increasing. Today's technologies such as Smart Home, Internet of Things and the ongoing digitalisation of all areas of work and life forces organisations of all sizes to invest more and more resources in maintaining the information security.

Building a security level for all business processes, information and IT systems that meets the actual needs requires more than procuring anti-virus programs, firewalls or data backup systems: A holistic concept is the basis and the starting point for developing a sustainable security management. Information security management, or short IS management, is the element of general risk management that aims to ensure the confidentiality, integrity and availability of information, business processes, applications and IT systems. This is a continuous process in which strategies and safeguards are constantly reviewed and adjusted to changing requirements.

Information security is not only a question of technology but rather depends substantially on the organisational and personnel environment. The IT-Grundschutz takes this into account by describing both technical and non-technical security requirements for typical business areas, applications and systems according to the state of the art in the publications. In this context the focus is on practical security requirements with the objective of keeping the initial barriers to the security process as low as possible and avoiding too complex approaches.

Introductory guide to information security

The present guide for the IT-Grundschutz Methodology "Basic Protection" provides a compact and clearly structured introduction to the development of an information security management system (ISMS) in an organisation. An ISMS is a planned and organised course of action to achieve and maintain an appropriate level of information security. The guide is based on BSI Standard 200-2 regarding the IT-Grundschutz Methodology and explains elementary steps for reviewing and increasing the information security level.

BSI Standard 200-2 describes how the IT-Grundschutz Compendium can be used to establish an efficient management system for information security. The approaches according to IT-Grundschutz combined with the IT-Grundschutz Compendium provide a systematic methodology to develop security concepts and tried and tested security safeguards that have been successfully implemented by numerous government agencies and companies for many years.

Basic Protection enables the implementation of comprehensive, basic initial safeguards across all business processes and/or specialist procedures of an organisation as a first entry point into the IT-Grundschutz. The approach is recommended for organisations that meet the following criteria:

- The implementation of information security is still at its beginning, and has a rather low level.
- The business processes do not have a significantly elevated risk potential regarding their information security.
- The aspired security level is normal.
- There are no assets, i.e. digital or analogue values, the theft, destruction or compromising of which would cause damage threatening the existence of the organisation.

- Minor security incidents can be tolerated – that means such incidents which despite costing money or otherwise causing damage do not threaten the existence.

Basic Protection allows the prompt implementation of the most important security requirements. Based on this, the security level can be further increased at a later time, for example, by protecting all areas with the Standard Protection or critical business processes with the Core Protection.

Basic Protection thus provide a feasible introduction to information security as part of daily practice – also and particularly – for small and medium-sized enterprises. Basic initial safeguards can be implemented very quickly with relatively low effort.

Decision for Basic Protection

In addition to the Basic Protection, the IT-Grundschutz Methodology provides two other approaches which can be implemented depending on an organisation's individual security requirements. Those responsible for information security can thus choose between the Basic, Standard and Core Protection.

The Basic Protection enables the first steps towards a security management in order to reduce the greatest risks as quickly as possible, whereas the Core Protection serves for the protection of elementary business processes and resources.

When Basic Protection has been successfully implemented for an organisation, the Standard or Core Protection should follow as a next step towards a solid information security. In the best case, the complete Standard Protection based on BSI Standard 200-2 is implemented over time, which corresponds to an updated approach based on the previous BSI Standard 100-2.

Target group

In general, the guide is aimed at those who implement the information security in companies. Typically these are Information Security Officers (ISO). In smaller organisations, where the area of information security has not been professionally developed to such an extent (yet), other employees may initially assume this task. Suitable are, for example, employees from the areas Finance and Controlling, IT operation or the corporate data protection officer, however, due to their original task and potential role conflicts with restrictions only.

Basic Protection: Added value for information security

The guide to Basic Protection provides those responsible with the required know-how to review the level of information security of an organisation, to identify vulnerabilities and to improve the security by means of suitable safeguards. The Basic Protection allows a clear and very practicable course of action for implementing initial safeguards. The holistic approach of the IT-Grundschutz Methodology, which, in addition to technical aspects, also considers infrastructural, organisational and personnel aspects, can be used to protect business-relevant information and data against misuse and access from third parties.

2 Information security management with IT-Grundschutz

The BSI Standard 200-2 describes how an efficient management system for information security can be set up and how the IT-Grundschutz Compendium can be used for this task. The approaches according to IT-Grundschutz combined with the modules of the IT-Grundschutz Compendium provide a systematic methodology to develop security concepts and tried and tested security safeguards that are successfully being used in numerous government agencies and companies. Using the Basic Protection approach of BSI Standard 200-2, the present guide schematically explains the process for establishing an ISMS and how this can be continued.

Overview of the information security process

In order to achieve an appropriate level of security a systematic approach is required for designing the security process.

The holistic implementation of information security in a single large step has often proven to be a too ambitious aim. Many small steps and an ongoing, continuous process are often more successful.

A high investment at the beginning is often not required. It can thus be better to implement the urgently required security precautions initially only within selected areas. This approach corresponds to Basic Protection. Once the most urgent security issues have been addressed, all further aspects in the overall organisation can subsequently be reviewed and improved.

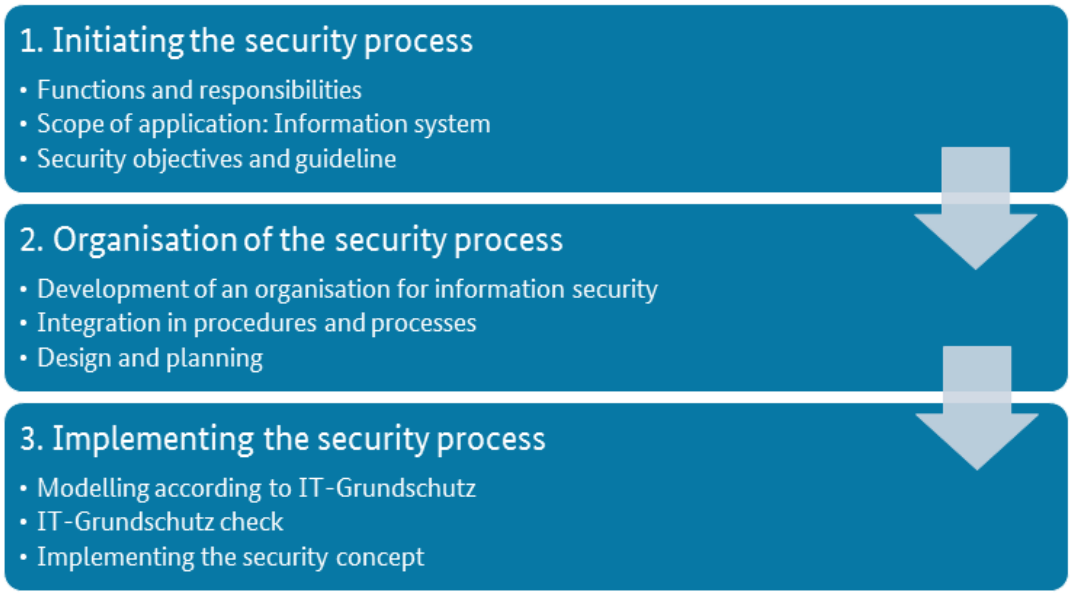


Figure: Three steps to information security

The present guide shows how Basic Protection can be implemented in three steps. The steps are based on the phases of the security process according to the IT-Grundschutz Methodology.

Some of these phases can be performed simultaneously, for example, designing and planning the security process can take place at the same time as establishing the information security organisation. In this case the advance phases must be updated later to take the new results into account.

In the following, the steps of the security process are briefly described.

1. Initiation of the security process

The management level must initiate, control and monitor the security process. This requires strategic guiding statements regarding the information security, on the one hand, and general organisational conditions, on the other. The Information Security Officer (ISO) plays the central role in this process.

An essential basis for the design of the security process is the Policy for information security. It describes for which scope the organisation envisages which security objectives and which security level, what the motivation is for this and with which safeguards and which structures this is to be achieved.

2. Organisation of the security process

An organisational structure suitable for the size and type of the organisation has to be established for the information security management. For this purpose, interfaces, communication channels and processes for cooperation have to be defined. In case of very small companies this should be as uncomplicated as possible.

3. Implementing the security process

Once an information security process has been initiated and the security policy and information security organisation have been defined, the security conception for the organisation can be developed in the next step. As a basis, the modules of the IT-Grundschutz Compendium contain corresponding security requirements according to the state of the art for typical components of business processes, applications, IT systems and other objects. These are structured thematically and can be build on each other.

The IT-Grundschutz Methodology reduces the analytical effort to a gap analysis approach between the security requirements from the relevant modules and the safeguards already realised in the organisation. Requirements that are found to be missing or inadequately implemented reveal security deficits that can be rectified by consequently implementing the derived safeguards.

Maintenance and improvement of information security

The aim of security management is to achieve an aspired level of security and to permanently maintain and, in the best case, continuously improve it. Therefore, the process itself and the organisational structures for information security must be checked at regular intervals for their adequateness, effectiveness and efficiency. The same applies to the chosen safeguards. After completion of the initial safeguards, the approach should be supplemented or extended, for example, from Basic Protection to Standard Protection or by using Core Protection.

3 Drawing up of a security concept according to the Basic Protection approach

This chapter describes in detail how a security concept can be implemented in three steps according to the Basic Protection approach.

3.1 Initiation of the security process

This chapter describes the first steps for implementing Basic Protection in an organisation. The responsibility for this is borne by the management. In addition, the Information Security Officer (ISO) assumes a central role, as the focus is on defining the security objectives in form of a guideline already at this point in time.

3.1.1 Management decision: Responsibility of management

The top management level is responsible for ensuring that all business areas operate smoothly and properly and that risks are recognised early and minimised. With the increasing dependence of the business processes on information processing, the requirements to ensure internal and external information security also increase.

The management must initiate, control and monitor the security process. They decide on how risks are handled and provides resources. The responsibility for information security remains with the management. The operative task "information security", however, is usually delegated to an information security officer.

In the introductory phase of the security process, it is quite often the case, that no security organisation has been established and the later ISO has not been appointed yet. However, to initiate the security process, at least one person responsible for information security must be appointed who performs the initial steps for designing and planning.

It is recommended that the responsible persons constantly inform the top management level about potential risks and consequences due to the lack of information security. Following a security incident, the management of the company or government agency must be informed about potential risks promptly. On the other hand, the management must ensure that all decision-relevant information is obtained in due time.

At a glance: Security-relevant topics for the management level
• Security risks for the organisation and its information
• Impacts and costs in the event of damage
• Impacts of security incidents on critical business processes
• Security requirements resulting from statutory or contractual stipulations
• Typical approaches to information security in the industry
• The current level of information security in the organisation with the derived recommendations for action

The management bears the responsibility for achieving the security objectives, whereas the operative implementation and control of the security process is the responsibility of an ISO. All employees of an organisation must play their part in achieving the security objectives.

Above all, the management level must ensure that information security is integrated into all relevant business processes, specialist procedures and projects. Experience has demonstrated that the ISO requires the full support of the management of the company or government agency in order to be integrated by the relevant specialists responsible.

The management must set the objectives both for information security management and other areas so that the aspired security level is achievable in all areas with the resources provided (HR, time, finance).

At a glance: Management level responsibility

- The management level bears the overall responsibility for information security.
- The management level must be informed about potential risks and consequences for the information security at all times.
- The management level initiates the information security process within the organisation and appoints a responsible Information Security Officer (ISO).
- The management level supports the ISO unconditionally and provides sufficient resources to be able to achieve the set objectives.

3.1.2 Central role: The Information Security Officer (ISO)

An organisation must have a point of contact for all aspects regarding the subject information security. Only a central point of contact can solve a current problem: In day-to-day business, aspects of information security are often neglected, and in some organisations they are simply forgotten. If the responsibilities are not or not clearly assigned there is a risk that information security generally becomes "other people's problem".

This is where the role of the Information Security Officer starts. The ISO coordinates the task of “information security”, identifies vulnerabilities and works on improving the security level. There are various designations for this function in administrative and business organisations: Frequent titles are also Chief Information Security Officer (CISO) or Information Security Manager (ISM). In some organisations, the designation IT Security Officer is also used. However, ISO is the most appropriate designation here. It makes clear that the responsible person does not only take care of safeguarding IT-related aspects, but also of the protection of all types of information.

It depends on the type and size of the organisation if and how many additional employees have security roles.

Responsibilities and tasks

The ISO is responsible for managing all information security issues within the organisation. The ISO’s main task is to advise the management of the government agency or company in the performance of their tasks regarding information security and to support them in the implementation.

The ISO should be involved in all larger projects which could have significant impacts on information processing, in order to ensure that any security aspects in the different project stages are observed. For example, the ISO should be involved in the planning and introduction of new applications and IT systems as well as in major changes to the infrastructure or the outsourcing of business processes. Production systems and other equipment with IT or Internet functionality should also not be forgotten. In order to perform these tasks, it is desirable that the Information Security

Officer has knowledge and experience in the issues relating to information security and IT. The ISO should also have knowledge of the organisation's business processes.

Simultaneous role of Data Protection Officer

A frequent question is whether the role of the Information Security Officer can also undertake the role of Data Protection Officer. The two roles are not fundamentally mutually exclusive, but some issues need to be clarified in advance:

- The interfaces between the two roles should be clearly defined and documented.
- Direct reporting paths to the management level should exist for both roles.
- It must be ensured that adequate resources to undertake both roles are available. If necessary the post-holder must be supported by appropriate personnel.

It should not be forgotten that the Information Security Officer also requires a qualified deputy.

It is generally recommended to appoint one responsible contact person each for both subjects – information security and data protection. Similar to the ISO, the Data Protection Officer should accompany all aspects of data protection within an organisation and introduce appropriate control mechanisms. Both work closely together in their roles and report to the management level.

At a glance: Responsibilities & tasks of the ISO

- Managing the information security process and being involved in all tasks relating to it
- Providing management with support when creating the policy for information security
- Coordinating the creation of the security concept, the contingency planning concept and security policies and issue additional policies and rules for information security
- Initiating and monitor the implementation of security safeguards
- Informing management of the current status of information security
- Coordinating security-relevant projects
- Investigating security incidents
- Initiating and coordinating awareness-raising and training measures for information security

3.1.3 Scope for the security concept: the information system

The area of the organisation for which Basic Protection is to be implemented is referred to as scope or “information system”. An information system comprises all the infrastructural, organisational, personnel and technical components which serve to perform tasks in a particular field of information processing. An information system may comprise the entire information processing of an organisation, but also individual areas defined by organisational or technical structures (e.g. department networks) or shared business processes or applications (e.g. HR information system). For the application of Basic Protection it must be defined how the information system to be protected should look like. It is important that the business tasks and processes under review are completely included in the scope. In particular in larger organisations defining the scope is not a trivial task. Organising by areas of responsibility can be helpful for defining the scope. For Basic Protection, the scope usually comprises the entire organisation.

Not only technical, but also organisational aspects should be considered when defining the scope, so that the areas of responsibilities and competences can be clearly defined. In any case it should be clear which information, specialised tasks or business processes are explicitly considered in the security concept.

The following aspects should be taken into account when defining the information system:

If possible, the scope should comprise all areas, aspects and components which serve for supporting the specialised tasks, business processes or organisational units and which are administrated within the organisation.

If this is not possible, because the organisation of parts of the specialised tasks or business processes considered depends on external partners, for example, within the scope of outsourcing, the interfaces should be clearly defined, so that this can be taken into account within the scope of the security concept.

Important aspect: Outsourcing

The outsourcing of business and supporting processes, such as, for example, the IT operation continues to be viewed with criticism by many experts. In smaller organisations, a well planned outsourcing project can nonetheless contribute to increasing the level of information security. This applies in particular, if outsourcing solutions or the purchase of external services is used to compensate for expert knowledge missing in the organisation. However, for outsourcing solutions to have a positive impact on the information security, some rules have to be observed: Before the outsourcing of business processes, it must be clarified whether this might not be advisable for security reasons. One reason could be, for example, insufficiently guaranteed protection of confidential data.

Once a decision for an outsourcing solution has been taken, the essential security requirements for the project must be defined. These form, among other things, the basis for choosing an outsourcing service provider. As part of this process, proof of the information security in the organisation and the qualifications of the employees should be obtained. Certificates such as IT-Grundschutz or ISO 27001 may be useful indicators for a certain security level.

When drafting a contract with an outsourcing service provider, the security requirements and criteria regarding service quality and security must be described with the highest possible level of detail. The contract should also include provisions regarding the obligation to provide information, the duty to cooperate and the obligation to carry out audits.

In addition, the contractor and the outsourcing service provider must agree a detailed security concept including a contingency concept. During transfer of the tasks, the areas of responsibility must be defined and a contact person must be appointed on both sides. The contractor must also carry out regular checks for maintenance of the information security at the service provider or have such checks carried out by a third party during the outsourcing project. Before completion of an outsourcing project, the rights of ownership to the hardware and software as well as the return of the data from the service provider should be clarified.

Information security is a fundamental subject which should be addressed at an early stage when choosing possible outsourcing service providers. In negotiations consisting of several stages with different providers internal risk assessments can make the choice easier. It will however not be possible to implement every security feature from the requirements specification at an acceptable price. Additional information on the subject of outsourcing can be found in the IT-Grund-schutz Compendium, in particular in module OPS.2 *Operations of third parties*.

At a glance: Defining the information system

- Define which critical business processes, specialised tasks or parts of the organisation should be included in the scope.
- Clearly define the scope.
- Describe interfaces to external partners.

3.1.4 Drawing up a policy for information security

The policy for information security serves as a starting point for the planned analysis of the requirements for information security in the own organisation. In this policy, the objectives and means for achieving a higher security level should be defined in general terms. In addition to the aspired information security objectives, it also contains the basic security strategy. The policy also describes the level of security aimed at in a government agency or company beyond the security objectives. It is therefore both a requirement and a statement that a specific security level should be obtained at all levels within the organisation.

Responsibility of the organisation's management for the security policy

The policy on information security documents which strategic positions the organisation's management provides for achieving the information security objectives.

Since the security policy represents a central strategy paper for the information security in an organisation, it must be worded and prepared such that all addresses can identify with its content. The ISO should thus involve as many areas as possible in the creation of the policy. The following organisational units can be involved, for example: Specialists responsible for important applications, IT operation, security (information, IT and infrastructure security), the Data Protection Officer, production and manufacturing departments, the HR department, the personnel representative, audit, representatives for financial issues or the legal department.

Formulating general information security objectives

At the beginning of every security process, the information security objectives should be carefully determined in accordance with the specific requirements. Specific security requirements for handling information are derived from these when creating the security policy and later when creating the security concept and designing the information security organisation.

In order to be able to define the security objectives, estimates should first be made on which business processes, specialist procedures and information are essential for the task fulfilment and which value these are assigned. In this respect, it is important to clarify to what extent the task fulfilment within the organisation depends on the core values confidentiality, integrity and availability of information and the IT employed. These statements will play a key role throughout the security process when selecting security safeguards and strategies.

This process step does not require a detailed analysis of the information system. As a result it should be possible to make a statement on which values or processes are of particular importance for the organisation and to specify the reasons for that.

At a glance: Examples of security objectives

- High reliability for actions, and for handling information in particular (availability, integrity, confidentiality)
- Ensuring the good reputation of the organisation in the eyes of the public
- Preserving the value of investments in technology, information, work processes and knowledge
- Protecting the high and possibly irretrievable value of information processed
- Satisfying the requirements resulting from statutory provisions
- Protecting individuals with regard to their physical and mental integrity

Content of the security policy

The security policy should be formulated clearly and concisely. More than ten pages are rarely necessary. The final version of the policy agreed between ISO and management should be brought to the attention of all employees and published at a central location, for example, on the intranet. After all, every employee should be involved actively in the task of "information security". In this context, the security policy makes an important contribution to increasing the awareness for information security within an organisation.

The following overview shows the basic contents of a security policy:

- importance of information security and significance of the relevant information, business processes and IT for the task fulfilment
- reference of information security objectives to the business objectives or tasks of the organisation
- security objectives and the key elements of the security strategy for the business processes and the IT employed
- assurance that the security policy will be implemented by the organisation's management
- guiding statements for success monitoring
- description of the planned organisational structure
- tasks and responsibilities in the security process should be set out
- programmes to promote information security via training and awareness-raising activities may be announced
- important threats, relevant statutory regulations etc. can be outlined at the beginning.

Due to the changing business objectives and processes, it is advisable to review and update the security policy at regular intervals and/or due to special events.

At a glance: Drawing up a security policy

- Identify organisational units to be involved for the security policy
- Define the scope and contents together
- Organise implementation of the security policy by the management level
- Announce the security paths
- Regularly check and if necessary update the security policy

3.2 Organisation of the security process

In order to achieve and to maintain an appropriate and adequate level of information security in the organisation, a planned course of action and an adequate organisational structure are indispensable. Furthermore, it is necessary to define security objectives and a strategy for achieving them as well as to ultimately set up a continuous security process for maintaining the security level that has been achieved.

3.2.1 Establishment of an organisation for information security

The aspired security level can only be achieved, if the requirements from the information security process are implemented consistently across the entire scope of the policy. Due to this condition, it is necessary to define roles within the organisation which assume the responsibility for implementing the processes. The employees should be adequately qualified in all aspects of information technology and information security. This is the only way to ensure that all important aspects are taken into consideration and that all tasks are performed.

The organisational structure required to promote and implement the information security process is referred to as the information security organisation, or short IS organisation. The composition of an IS organisation depends on the size, nature, and structure of the particular organisation. The ISO should generally be appointed as the central point of contact for the coordination, administration and communication of the information security process. In larger organisations, there are also often employees who assume subtasks in the area of information security.

The roles should have direct access and directly report to the management. At management level, the information security role should be assumed by a responsible manager to whom the ISO reports.

Regardless of how an optimal structure for one's own IS organisation is to be designed, the following basic rules should be observed in any case.

Basic rules when defining roles in the information security management

- The management level has the overall responsibility for the correct and secure fulfilment of tasks.
- At least one person must be appointed as an ISO who coordinates and controls the information security process.
- All employees are equally responsible for both, their original tasks and for maintaining the information security at their place of work and in their environment.
- Information security must be integrated in the processes within the overall organisation and contact persons must be specified. The aim is that the necessary security aspects are taken into account in all strategic decisions at an early stage.

As risks for information security as well as IT risks are among the most important threats for the operational day-to-day business, the methods for information security management should be coordinated with the already existing methods for handling risks in other areas. Detailed information on this subject can also be found in BSI Standard 200-3 "Risk analysis based on IT-Grund-schutz".

Structure of the information security organisation

Depending on the size of an organisation, there are different options for designing an organisational structure for an information security management. The figure below shows the structure of an IS organisation in a small organisation. The ISO here cooperates closely with the management, the relevant specialists responsible and the Data Protection Officer of the company. The ISO acts as an interface between the other parties involved. The IS guidelines and specifications have been coordinated with the other responsible parties and published under the guidance of the ISO. They form the basis for how all employees deal with the subjects of information security.

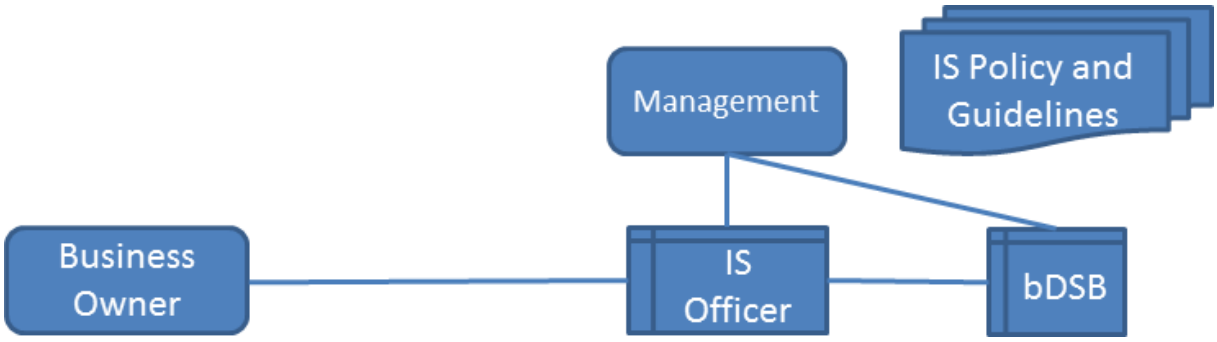


Figure: Structure of the IS organisation in a small organisation

Interaction with other organisational units and management disciplines

In most organisations, in addition to information security management, there are other areas that undertake tasks relating to information security or are entrusted with similar subjects. A coordinated approach and the definition of interfaces are indispensable, particularly given the fact that these areas are often organised as separate disciplines and, in some instances, in other organisational units. They have in common that they pursue the aim of protecting values of the organisation. In addition to information security management, this includes the subjects of data protection, protection of objects, protection of persons, protection of classified information, business continuity management or risk management. In organisations with a production area, cooperation with the persons responsible for product and plant safety is also important.

Collaboration with the IT operations department

Many subtasks of security management are directly linked to tasks of the IT operations department. The ISO issues specifications for the safe operation of IT systems and networks, which the IT operations department has to implement. Therefore, the security management and the IT operations department have to work closely together and regularly exchange information about approaches, current threats and new security requirements. In larger organisations, it can thus be appropriate to appoint a dedicated contact person for the ISO in the IT operations department.

At a glance: Organisation of the security process
• Stipulate roles for designing the information security process
• Assign tasks and areas of responsibilities to the roles
• Stipulate the human resources required for the roles
• Document the IS organisation
• Integrate the information security management into the processes

3.2.2 Designing and planning the security process

For the further steps in the security process, all relevant framework conditions should be identified. To this end, the most important business processes and specialised tasks as well as the level of information security they require should be determined.

The determination of the framework conditions is an important basis for further considerations regarding information security: Already at this point of the process, it can be noticed if relevant information is missing and an initial estimation of the aspired security level becomes possible. During review of the current level of information security by employees of the organisation, often information about which organisational and infrastructural areas have a need for optimisation is revealed, along with the technical requirements.

General influencing factors

An adequate level of Information security is one of the major preconditions for organisations to achieve their business objectives. Therefore, the following influencing factors must be considered:

- **Business objectives**: Which factors are essential for the success of the company or government agency? Which products, offers and contracts form the basis of the business activities? What are the general objectives of the organisation? What is the role of information security in this?
- **Organisational structure**: How is the organisation organised and structured? Which management systems exist (for example, risk management or quality management)?
- **Cooperation with external parties**: Who are the most important customers, partners and committees? What are their basic requirements and expectations regarding information security of the organisation? Who are the most important service providers and suppliers? What is their role for the organisation's information security?
- **Strategic context**: What are the major challenges for the organisation? How is the competitive position?

Framework conditions – internal and external

Many internal and external framework conditions may affect information security and must therefore be determined. By analysing the business processes (including specialised tasks) statements regarding the potential impacts of security incidents on the business activities and the task fulfilment can be derived. In many organisations, overviews for business processes, objects or data collections required for operation aspects or administration already exist. If available, ex-

isting process landscapes, business distribution plans, databases, overviews, network plans and inventory tools can be used to identify the essential business processes. In taking these overviews into account, it should be ensured that the records don't become too detailed. The aim is an initial general overview of which information is processed for a business process with which applications and IT systems. This can be used as a basis for taking further decisions.

At a glance: Clarifying important internal and external framework conditions

- Which business processes exist in the organisation and how are they connected to the business objectives?
- Which business processes are dependent on a functional information technology?
- Which information is processed for these business processes?
- Which information is particularly important and thus worthy of protection with regard to confidentiality, integrity and availability, and why (e.g. personal data, customer data, sensitive internal company information)?
- A responsible contact person must be appointed for every business process and every specialised task.
- What is the legal framework (national and international laws and regulations)?
- How do the customer, supplier and partner requirements, the current market situation, competitive situation and other relevant market-specific dependencies look like?
- What are the industry-specific security standards?

Brainstorming: Determination of the framework conditions

In order to determine all framework conditions for the essential business processes as quickly and comprehensively as possible, it is recommended to carry out a short brainstorming for every business process. These meetings should be led by the ISO with the relevant specialists responsible and the relevant person responsible for IT.

The focus of the internal determination should predominantly be on business-critical information and core processes as well as the associated applications, IT systems, networks and rooms. Based on the core processes, the main supporting processes and the mainly affected objects should be determined in addition.

Initial recording of the processes, application and IT systems

The results of the previous steps, i.e. the determined framework conditions and the formulated information security targets should now be consolidated with the organisation's existing values in an overview.

As in most cases an information system consists of a large number of individual objects, it is often not appropriate to record every object individually. Instead, it has proven useful in practice to summarise similar objects into groups. It is also possible to draw up a graphic network overview first and use this as a basis for recording the IT systems. The representation of the network overview may be highly simplified. IT systems or processes that have been outsourced or are operated in the Cloud should also be listed here.

The initial recording should only include the essential objects. For example, server rooms, which in most cases have a higher security level should be included, whereas the traditional office

rooms should not. The result of the initial recording should be an overview which can be created with relatively limited resources.

At a glance: Determining the relevant objects

- Business process or specialised task:
  Name and (if required) description, responsible specialist
- Application:
  Name, (if required) description and associated business process
- IT, ICS systems and other objects:
  Name, platform and installation location, where appropriate
- Rooms relevant for operation, which require an increased security level (e.g. server rooms):
  Type, room number and building
- IT systems and networks should be recorded as physical structures and clearly marked

Estimation of the security level

For future considerations, it may prove useful to estimate the aspired security level of the individual assets, i.e. the target objects, at an early stage. This initial estimation of the security level provides a rough orientation for the expected time and expense and facilitates classifying the identified assets into groups.

The objects identified so far, for which a higher security level is aspired as "normal" should be marked in the table already prepared.

Creating a graphical network plan

Based on the information captured, a rudimentary network plan should be created to provide a better overview. This network overview can facilitate the further discussion and reveal whether essential IT systems were overlooked. The plan should contain the following objects as a minimum:

- IT systems, i.e. clients and servers as well as active network components
- Network connections between these systems
- Connections of the area under consideration to the outside.

The graphical network overview should not only contain physical components, but also virtualised structures. In this respect, virtual structures can either be directly included in the network overview, or entered in a separate network overview in case of more complicated architectures. The same applies to such IT systems and processes that are outsourced. An example for initial recording including a network overview can be found in the Resources for IT-Grundschutz on the BSI website. The results obtained here will be specified in more detail and completed in the structure analysis to be subsequently performed.

At a glance: Designing and planning the security process

- Appoint contact persons for all business processes and specialist tasks
- Perform basic assessment on the value and security level of information, business processes and specialist tasks
- Determine internal and external framework conditions
- Estimate the importance of business processes, specialist tasks and information
- Set general information security objectives
- Draw up a consolidated overview of the existing assets based on the knowledge gained previously

Documentation in the security process

Decisions should always be comprehensible and repeatable. Therefore, a large number of different documents is prepared before and during the security process. In this respect, it should always be ensured that the time involved in the preparation of documentations remains within reasonable limits. If something needs to be documented during implementation of the IT-Grundschutz Methodology it is usually not necessary to create new documents. In general, it is sufficient to collect and/or record the information at a suitable location.

In particular for Basic Protection, the documentation process should be kept as simple and practical as possible.

3.3 Implementing the security process

Once the security process has been initiated and all organisational tasks have been completed, the last phase of the Basic Protection process already begins: the creation and implementation of the security concept.

For the security concept, organisational, personnel, infrastructural and technical requirements from the IT-Grundschutz Compendium should be met for typical components of business processes, applications and IT systems. These are described in the different modules according to subject, which allow for a modular approach. For implementation of Basic Protection, only the basic requirements need to be observed.

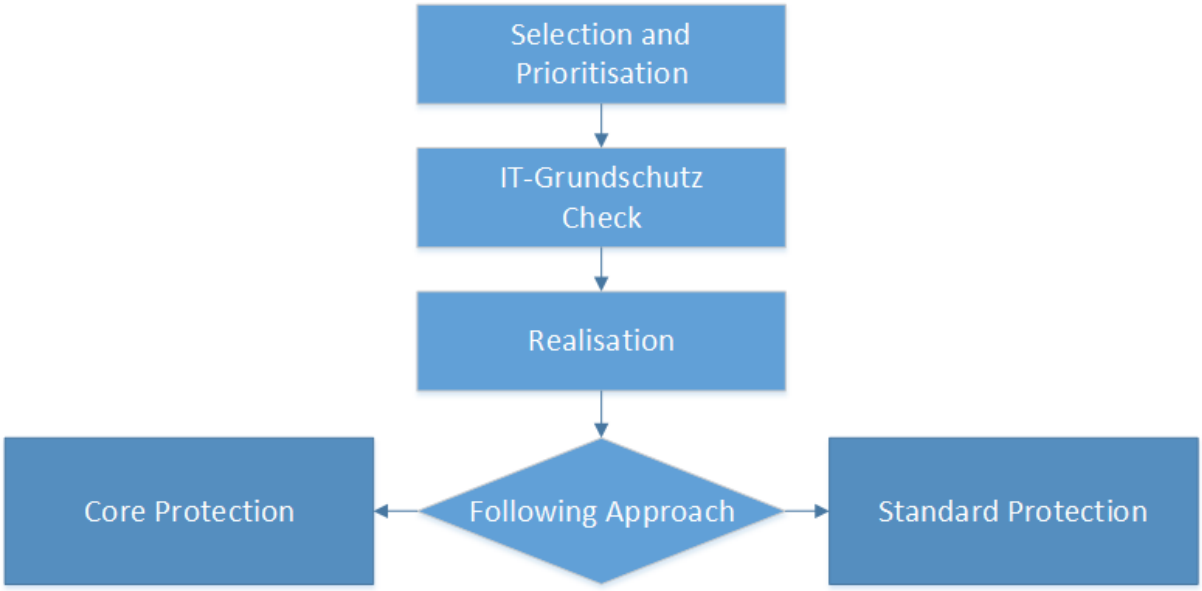


Figure: Schematic approach according to the Basic Protection concept

After the scope has been defined in the previous step of organising the security process, the creation of a security concept following the implementation of Basic Protection is divided into the following fields of action, which will be described in more detail in the following:

- **Selection and Prioritisation**:

  The information system under consideration should be mapped with the help of the modules from the IT-Grundschutz Compendium.

- **IT-Grundschutz Check**:

  In this step, it is checked whether and to what extent the specifications in the basic requirements according to IT-Grundschutz are already met and which security safeguards are still missing.

- **Realisation**:

  Suitable security safeguards have to be defined and implemented for the basic requirements not yet met.

- **Choice of the following approach**:

  The Basic Protection is intended as an initial approach. It must thus be defined at which time and with which IT-Grundschutz approach the security level is to be increased further.

3.3.1 Selection and prioritisation of the modules (modelling)

As a first step, the information system under consideration is mapped on the basis of the processes, applications, IT systems, communication connections and rooms identified in the initial recording and the existing modules from the IT-Grundschutz Compendium. The result is an IT-Grundschutz model of the information system which consists of different modules, which might have been used several times, and thus contains the security-relevant aspects of the information system.

Modelling according to IT-Grundschutz

In order to model an often complex information system according to IT-Grundschutz, the corresponding modules from the IT-Grundschutz Compendium have to be selected and implemented. For improved manageability the modules in the IT-Grundschutz Compendium are divided into process- and system-oriented modules as well as different layers. Further details on the structure and the contents can be found in the Appendix “The IT-Grundschutz Compendium – Everything you need to know at a glance".

Modelling according to IT-Grundschutz now consists of selecting modules or individual aspects for mapping the information system. Depending on the module, the target objects may be different: individual business processes or components, groups of components, buildings, premises, organisational units etc. If individual target objects cannot be mapped with the modules, comparable or higher-level modules must be used instead.

Order of module implementation

In order to minimise basic risks and to establish a holistic information security system, it is necessary to meet the essential security requirements and to implement corresponding security safeguards at an early stage. The IT-Grundschutz Methodology therefore recommends a specific order when implementing the modules. The chapter “Layer model and modelling” of the IT-Grundschutz Compendium describes when it is appropriate to use an individual module and which target objects it should be applied to. The modules are marked accordingly to indicate the priority of their implementation.

This marking provides a sensible temporal order for implementation of the relevant requirements, however, it does not weight the modules among each other. In general, all relevant modules from the IT-Grundschutz Compendium must be implemented for an information system. Every organisation can define a differing order, as appropriate for them.

Whether the information system consists of already used components or whether it is an information system that is still in the planning stages is not relevant for the IT-Grundschutz model created. The model can thus be used in different ways:

- The ISO can use the IT-Grundschutz model of an existing information system to identify relevant security requirements based on the modules. It can be used in the form of a **test plan** to perform a gap analysis.
- On the other hand, the IT-Grundschutz model of a planned information system constitutes a **development plan**. Using the selected modules, it describes which security requirements need to be met when the information system is realised.

The position of the modelling phase and the possible results are illustrated in the following diagram:

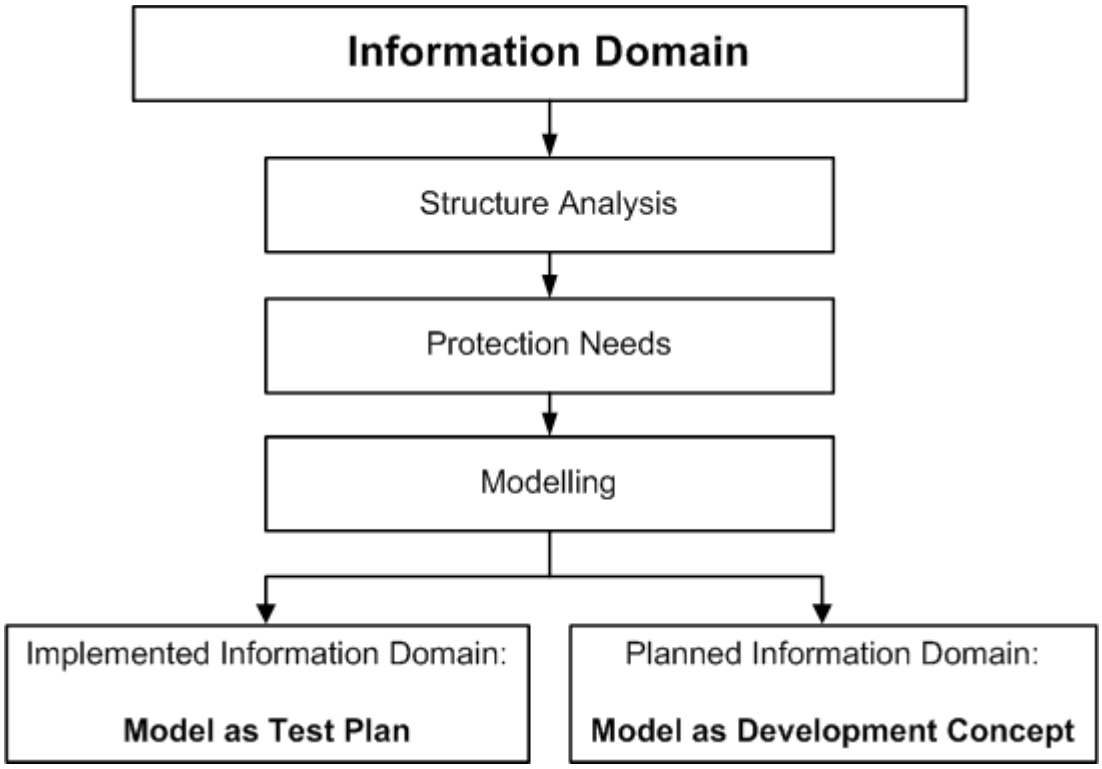


Figure: Results of modelling according to IT-Grundschutz

In general, an information system contains already existing as well as planned parts so that the resulting IT-Grundschutz model contains a test plan as well as parts of a development plan. Therefore, all security requirements together form the basis for creating the security concept:

- security requirements already met,
- requirements identified as inadequately met or not met at all during the gap analysis, and
- requirements arising for the parts of the information system that are still being planned.

Assignment of modules

The assignment of modules to target objects should be documented in the form of a table containing the following columns:

- Complete title and number of the module (e.g. SYS.3.1 Laptop)
- Target object or target group: For example, this could be the identification number of a component or a group or the name of a building or organisational unit
- Contact person: This column serves initially only as a placeholder. The contact person is not determined at the modelling stage, but only at the point when the gap analysis in the IT-Grundschutz Check is being planned
- Order: The implementation order (R1, R2, R3) of the module should be entered.
- Notes: Additional information or the rationale behind the modelling can be documented in this column

At a glance: Modelling an information system

- Systematically work through the "Layer model and modelling" section in the IT-Grund-schutz Compendium.
- Determine the target objects in the information system under consideration to which each module in the IT-Grundschutz Compendium is to be applied.
- Document the assignment of modules to target objects ("IT-Grundschutz model") and the relevant contact persons.
- Note target objects that cannot be modelled appropriately.
- Define an order for the implementation of the modules.

3.3.2 IT-Grundschutz Check for Basic Protection

The selection and prioritisation of the IT-Grundschutz modules is referred to as the test plan in the following. Using a gap analysis, it is to be determined which basic requirements are met adequately and which only inadequately or not at all.

For an IT-Grundschutz Check for Basic Protection, only the basic requirements need to be met. For a potential future Standard or Core Protection, a separate IT-Grundschutz Check should be performed adding the standard requirements of the modules concerned. In order to avoid additional effort and to be able to use synergy effects, the results of the IT-Grundschutz Check for the Basic Protection should be prepared such that they can be integrated directly into the Standard or Core Protection at a later point in time.

The IT-Grundschutz Check consists of three different steps. The first step entails making the organisational preparations and selecting the relevant contact persons for the gap analysis. In step 2 the gap analysis is performed using interviews and sampling checks. In the final step, the results of the gap analysis are documented, together with the rationale behind it.

Step 1: Organisational preparations

A certain amount of preliminary work is required to ensure that the gap analysis proceeds smoothly. First of all, it is necessary to inspect all the in-house documentation which controls security-relevant processes, e.g. organisational instructions, work instructions, security instructions, manuals and "informal" approaches. These documents can be helpful in ascertaining the degree of implementation, especially for questions about existing organisational procedures. It is further necessary to clarify who is currently responsible for their content, in order to be able subsequently to determine the correct contact person.

It must then be established whether and to what extent any external parties need to be involved in ascertaining the implementation status. For example, this might be necessary if there are any external computer centres, external parent organisations or companies to which parts of business processes or the IT operations have been outsourced.

An important aspect is to determine suitable contact persons for the individual modules which were used for modelling the present information system. With the requirements in the modules, the roles that are responsible for the implementation are specified. Based on this information, the contact persons for the relevant subject matter in the organisation can be identified. Some examples for contact persons of the different areas can be found below:

- For the modules in the ORP, CON and OPS layers a suitable contact person will generally be found by means of the subject matter dealt in the module. For example, for the module ORP.2 *Personnel* the contact person should be an employee from the HR department. For the design modules, the person whose terms of reference include updating procedures in the area under consideration should be interviewed.
- For the layer INF the selection of suitable contact persons should be agreed with the general services and/or site technical services departments. Depending on the size of the organisation under consideration, different contact persons could be responsible, for example, for the infrastructural areas of buildings and technology rooms. In small organisations the caretaker will often be able to provide the information.
- In the system-oriented modules in the SYS, NET and IND layers, there is a heavy emphasis on technical aspects in the security safeguards to be checked. Possible contact persons are therefore generally the administrators of these components or groups of components.
- For the modules in the layer APP the persons responsible for the individual applications should be selected as the main points of contact.

Overview: Organisational preliminary work of the IT-Grundschutz Check

- Sift through internal documents for responsibilities and rules and clarify who is responsible for these documents.
- Determine to what extent external assistance is required.
- Define main contact persons for all the modules used in the modelling.

Step 2: Performing the gap analysis

Once all required preliminary work has been completed, the security requirements of the relevant module, for which the contact persons are responsible, are progressively worked through together with them. In addition, the purpose of the IT-Grundschutz Check should be briefly explained to the interviewees. If it is necessary to verify the statements made, this could be achieved, for example, by examining samples of the relevant regulations and concepts. In the case of infrastructure, for example, the objects under investigation could be visited together with the contact person on site. Also, client and/or server settings in selected IT systems could be checked together.

At the end, an agreement should be reached between the ISO and the relevant contact person regarding the implementation status.

The following statements are possible as answers to the implementation status of individual requirements:

"unnecessary" The requirement does not need to be met in the form suggested, because the requirement is not relevant in the information system under consideration (for example, because services were not activated) or has already been met due to alternative safeguards.

If the implementation status of a requirement is set to "unnecessary", the associated elementary threats have to be identified using the cross-reference table of the relevant module. If alternative safeguards have been implemented, it must be proven that the risk arising from all elementary threats concerned has

	been minimised appropriately. If basic requirements are not met, generally an increased risk remains present. Requirements must not be set to "unnecessary" by generally accepting or ruling out the risk for an elementary threat identified in the module using the cross-reference table.
"yes"	Appropriate safeguards have been implemented completely, efficiently and appropriately for the requirement.
“partially"	The requirement has only been partially implemented.
"no"	The requirement has not been met yet, i.e. appropriate safeguards have largely not been implemented yet.

It is useful to have the module texts as well as the implementation recommendations or other supplementary material at hand during the interviews.

Overview: Performing the gap analysis

- Prepare checklists in advance for each specialist area.
- Establish the implementation status of the individual requirements together with the contact person.
- If required, verify the implementation status by means of sample checks on the object.

Step 3: Documentation of the results

The results of the IT-Grundschutz Check should be documented such that all those involved can understand them, and they can be used as the basis for implementation planning for the identified safeguards.

For documentation of the IT-Grundschutz Check the following should be recorded:

- the number and name of the object or group of objects to which this module was assigned during modelling,
- the location of the assigned objects or group of objects,
- the date on which the information was recorded and the name of the author, and
- the contact person interviewed.

The results of the gap analysis should be listed in a table. In this context, the following information should be recorded for each requirement of the relevant module:

- **Degree of implementation** (unnecessary/yes/partially/no)

  The implementation status of the relevant requirement determined in the interview should be recorded.

- **Date for the implementation**

  This field is useful, even though it is generally not completed during an IT-Grundschutz Check. It serves as a placeholder which will be used during implementation planning to document the date by which the requirement should have been fully met.

- **Persons responsible**

  If, when performing the gap analysis, it is clear which member of staff will be responsible for fully implementing a requirement or safeguard not fulfilled yet, the name of this person should be documented in this field. Otherwise, a responsible person should be determined as part of the later implementation planning.

- **Notes/reason(s)**

  This field is important to be able to understand decisions made at a later point. In the case of requirements whose implementation appears dispensable, the rationale for this should be stated here. In the case of requirements that have not yet been implemented or only partially implemented, this field should document which safeguards still have to be implemented. Any other notes which will assist in eliminating deficits or which need to be considered in the context of the requirement should also be entered here.

- **Deficits/cost estimate**

  For requirements that have not yet been met or only partially met, the associated risk should be determined and documented in an appropriate form. In the case of such safeguards, an estimate of the financial and staffing resources that will be needed to eliminate the deficits should be made.

Forms which can be used as resources for documentation of the IT-Grundschutz Check are available for all modules of the IT-Grundschutz Compendium on the BSI website.

Overview: Documentation of results
• Collect master information for each target object
• Document information concerning the IT-Grundschutz Check and the implementation status
• Include fields or placeholders for implementation planning

3.3.3 Implementation of the security concept

The results of the IT-Grundschutz Check, i.e. a gap analysis, are available at this stage. This chapter describes how to plan, execute, supervise, and monitor the implementation of the required security safeguards. Exemplary implementation recommendations for security safeguards are available for many T-Grundschutz modules and can be used for implementing the requirements of the modules. They are based on best practices and many years of experience of experts in the field of information security. However, the safeguards from the implementation recommendations should not be considered binding, and can be supplemented or replaced by one's own safeguards.

There are usually only limited financial and personnel resources to implement the safeguards. The aim of the steps described below is thus to implement the planned security safeguards as efficiently as possible.

Defining specific safeguards for the requirements

Using the IT-Grundschutz Check as a basis, it should be evaluated in an overall view which requirements from the IT-Grundschutz modules have not been implemented or only partially implemented.

In the modelling step, the modules to be implemented for the individual target objects of the information system under consideration were selected. The requirements which typically have to be implemented for these components in order to achieve an appropriate security level are described in the modules. For implementation of the Basic Protection, only the basic requirements need to be observed. They are of such elementary importance that their implementation is essential for the safeguarding of the information system. In addition, fulfilling the basic requirements usually delivers good results with a comparably low use of resources, so-called quick wins. The standard requirements as well as the requirements in the case of high protection requirements are relevant for the approaches of the Standard and Core Protection. But also within the scope of Basic Protection, it may be viable to take a look at these requirements in order to further increase the security level.

The requirements in the modules are formulated briefly and concisely. They must be translated into practical security safeguards which are appropriate for the organisational and technical circumstances in the organisation and meet the relevant requirements.

The safeguards serve as action guidelines for the various participants in the security process. Therefore, they must

- be adapted to the relevant framework conditions and the terminology used in an organisation, and
- be sufficiently specific to be able to be applied in the information system under consideration, i.e. contain technical details, for example.

In general, the requirements of the IT-Grundschutz modules should always be implemented in a general sense. All changes with regard to the IT-Grundschutz Compendium should be documented for better traceability.

Implementation recommendations are available for many modules of the IT-Grundschutz Compendium describing detailed and tried and tested safeguards for the security requirements. On the one hand, these safeguards are formulated in a very general manner so that they can be applied in as many environments as possible, and on the other hand, they are described in great detail to facilitate their implementation..

The safeguards suggested in the implementation recommendations should also be adapted to the relevant framework conditions of an organisation. It can be appropriate, for example,

- to further specify safeguards, i.e. to add technical details, for example,
- to adapt safeguards to the terminology used in the organisation, i.e. to use different role names, for example, and
- to delete any recommendations which are not relevant in the area under consideration from safeguards.

It is also important to plan for measures accompanying the implementation. These include, for example, measures for raising awareness among employees to emphasise the concerns of information security as well as the necessity and the consequences of the safeguards.

In rare cases, it is possible that individual requirements of the elementary basic requirements cannot be implemented under the specific framework conditions, for example, if their implementation would cause essential problems in other areas. This may be the case, for example, if fire control and intrusion protection requirements are incompatible. In such cases, different solutions must be found and the circumstances clearly documented.

In order to be able to trace the procedure followed in drawing up and adapting the list of specific safeguards at a later point, it should be documented. If security requirements are added or modified, this must also be documented in the security concept. When selecting and adapting the security safeguards based on the requirements, it must be observed that they should always be appropriate. Appropriate means:

- **Effectiveness**: The safeguards must provide effective protection against the potential threats, i.e. cover the protection requirements identified.
- **Qualification**: They must be able to be implemented in practice, i.e. they may not, for example, excessively hinder organisational procedures or weaken other security safeguards.
- **Practicability:** They should be easy to understand, easy to apply and generally not prone to error.
- **Acceptance:** They must be easy to apply for all users and must not discriminate or impair anybody.
- **Cost-effectiveness:** An optimum result should be achieved with the resources used. This means that the security safeguards should, on the one hand, minimise the risk in the best possible manner, and on the other hand, be proportionate to the assets to be protected.

Estimating the time and expense

As the budget for implementing security safeguards is always limited in practice, the required investment costs and personnel expenses should be determined for each safeguard to be implemented. In this context, a differentiation should be made between one-time and recurrent investment costs and personnel expenses. At this point it is often revealed that savings on technical or infrastructural security safeguards often result in high ongoing labour costs. Vice versa, savings on personnel result in continuously increasing security deficits.

In this regard it is necessary to ascertain whether all the safeguards identified can be afforded. If there are safeguards which cannot be implemented at reasonable cost, it should be considered which alternative safeguards could be used to still meet the requirements. Often, there are different options to meet requirements with suitable safeguards. In this respect, it must be noted that normally basic requirements must always be met and that, due to their elementary nature, the acceptance of a residual risk is not provided for.

If estimates regarding costs and personnel expenses are available, it is usually still necessary to decide in detail how many resources are to be used for the implementation of the security safeguard. The results of the security review should thus be presented to the management of the organisation. These include the vulnerabilities determined (i.e. security requirements which are not or insufficiently met) as well as the costs and expenses to be expected for the implementation of the required safeguards. On this basis, the management can decide on the budget to be released.

If no sufficient budget can be made available for the implementation of all missing safeguards, the remaining residual risk should be determined. The cross-reference tables from the individual modules can be used for this purpose. The cross-reference tables provide an overview of which requirements counteract which elementary threats. Conversely, these tables can be used to determine for which elementary threats there is no sufficient protection, if requirements from the modules are not fulfilled. The resulting residual risks should be described in a transparent manner and submitted to management for a decision. The management level must assume the responsibility for the consequences.

Specification of the order of implementation of the safeguards

The IT-Grundschutz Compendium describes an order in which the modules should be implemented, from basic and comprehensive modules to such which cover more specific subjects and can thus be considered with less priority in respect to the time of their implementation. This order of implementation of the modules is particularly important when implementing Basic Protection. All safeguards derived from the basic requirements must be implemented for every module. However, it may also be useful to take a look at the relevant standard requirements and the requirements for elevated protection requirements, as these often describe and cover additional aspects.

If the existing budget or the staffing resources are not sufficient to be able to implement all the required safeguards immediately, a prioritisation must be determined here.

The further order of implementation is based on what is most appropriate for the relevant organisation. Here some tips:

- For some safeguards, there are dependencies and logical relationships that require a specific chronological order.
- The order of implementation can be based on when the relevant safeguards can be implemented within the life cycle of a target object. In the case of new target objects, for example, safeguards from the areas of planning and design should be implemented before such safeguards which deal with the secure operation. In the case of target objects which have been in the information system for a longer period securing the operation should be a priority.
- Some safeguards affect a large area, while the others have stronger local effects. It often makes sense to handle those safeguards affecting a large area first. However, it is also useful to weight the safeguards from the different areas according to how fast they can be implemented and to which security gain they provide. Quick wins can be often found in the organisational area or can be achieved by central configuration settings.
- The implementation of some modules has a larger impact on the desired security level than others. For example, safeguarding of servers should always come before safeguarding the connected clients.
- Modules, where a strikingly high number of requirements was identified as not met during the gap analysis, represent areas with many vulnerabilities. They should also be given preference.

Specification of the tasks and responsibilities

After determining the order for implementing the safeguards, it must be defined who will implement which and by when. The persons responsible must dispose of the necessary skills, competences and resources.

Likewise, it must also be specified who is responsible for monitoring the implementation and who is to be notified of the completion of the implementation of each safeguard. The reports are all gathered by the ISO, who is continuously informed about the progress of the implementation and the results. The ISO in turn must inform the management level on the progress and the resulting reduction of existing risks.

The implementation plan now completed should at least contain the following information:

- Description of the target object (operational environment),
- number and/or title of the module under consideration,

- title and/or description of the requirement to be met,
- description of the safeguard to be implemented and/or reference to the description in the security concept,
- implementation schedule,
- if available: dependencies and interrelations with other safeguards,
- available budget,
- persons responsible for implementation and
- persons responsible for overseeing the implementation.

Action points for implementation of the security concept

- Summarise missing or partially implemented IT-Grundschutz requirements or additional security safeguards
- Formulate security safeguards which meet the basic requirements
- Consolidate security safeguards, i.e. delete unnecessary safeguards, adapt general safeguards to the particular situation and check all safeguards for suitability
- Determine one-off and repeat costs and expenses for the safeguards that are to be implemented
- Determine suitable alternative safeguards for those that cannot be financed or provided
- Make a decision on which resources are to be used to implement the safeguards
- If necessary, highlight the residual risk and obtain a decision by the management level
- Stipulate, provide rationale for and document the implementation order
- Stipulate implementation deadlines and assign responsibilities
- Monitor the implementation and adherence to deadlines
- Train and raise awareness of affected employees

4 Information security is a process: Follow-up options

The implementation of Basic Protection is an important first step towards significantly increasing the level of information security in an organisation. It also establishes an initial solid base for the management system for information security. The selected security safeguards must be implemented further and specifications such as the security policy must be continuously updated to be able to maintain and to improve the information security process now started. This includes also to regularly review the IS process for its effectiveness and efficiency.

A regularly performance review and assessment of the process should be carried out by the management. For example, if the number of security incidents is increasing or in case of significant changes to the framework conditions, an additional review must be conducted between the regular ones. All results and decisions must be documented transparently. It is the task of the ISO to collect and to process this information and to inform the management.

By implementing Basic Protection, an organisation can achieve a good level of information security. In this initial process, many aspects have been considered, responsible specialists have been involved and the awareness of employees has been raised. However, given the highly complex and dynamic nature of information security, Basic Protection can merely be an initial starting point for addressing the subject: In the best case, the organisation continues the process with the two follow-up approaches from the IT-Grundschutz Methodology.

Core Protection

The focus of the Core Protection is initially on the business processes and assets at particular risk. This approach is recommended if an organisation largely meets the following criteria:

- The number of business processes with significantly elevated protection requirements is limited or only comprises a small part of all business processes of the organisation.
- The organisation is able to swiftly identify and clearly define those business processes having a significantly elevated risk potential regarding their information security.
- The organisation clearly owns identifiable assets the theft, destruction or compromising of which would cause damage threatening the existence of the organisation (so called crown jewels). These should be protected as a matter of priority.
- Minor security incidents, which cost money or cause other damage, but do not cause damage threatening the existence, are acceptable for the organisation.

Standard Protection

Standard Protection essentially corresponds to the classic IT-Grundschutz Methodology. Standard Protection provides an ISO with the means for comprehensive and in-depth safeguarding of the assets and processes of an organisation. Approaching the security process with Standard Protection is recommended, if the organisation largely meets the following criteria:

- The implementation of information security has reached a sufficient degree of maturity in the organisation, so that security safeguards already exist in key areas and no basic initial safeguards are required.
- There is no need to take action to safeguard individual business processes as a matter of priority, which have a significantly elevated risk potential regarding their information security (see Core Protection).

- The organisation does not have any assets the theft, destruction or compromising of which would cause an immediate damage threatening the existence and which therefore need to be safeguarded as a matter of priority.
- Security incidents, which conceivably impair the fulfilment of tasks, cost money or otherwise cause noticeable damage, are not acceptable for the organisation, even if they do not yet cause damage threatening the existence.

Within the IT-Grundschutz Methodology, the Standard Protection represents the approach which generally should be aspired in order to provide appropriate and comprehensive protection for all areas of an organisation.

By increasing the information security level, every organisation makes an important contribution towards improving the cyber security in Germany. The more professionals in companies and government agencies deal with the fundamentally important questions regarding information security and safeguards for protection and defence, the greater the gains for Germany's economy. The IT-Grundschutz with the updated contents in the BSI standards and the IT-Grundschutz Compendium provides comprehensive and practical solutions for companies of all sizes.

5 Appendix

5.1 The IT-Grundschutz Compendium – Everything you need to know at a glance

The IT-Grundschutz Compendium contains the IT-Grundschutz modules, in which different subjects of information security with regard to the specific threat scenario as well as security requirements are elaborated. It is made available online as the successor to the previous IT-Grundschutz Catalogues on an annual basis in the form of an updated edition.

The IT-Grundschutz modules

The IT-Grundschutz Compendium contains explanations regarding the threat scenario, security requirements, and additional information for different processes, components and IT systems, each summarised in a module. The Compendium has a modular structure and its focus is on representing the major security requirements in the modules. The aim is to be able to take new technical developments and version changes into consideration as early as possible thanks to this structure. Individual modules can thus be extended and updated as required. According to the basic structure the modules are divided into process- and system-oriented modules, and they are also categorised in a layer model according to subjects.

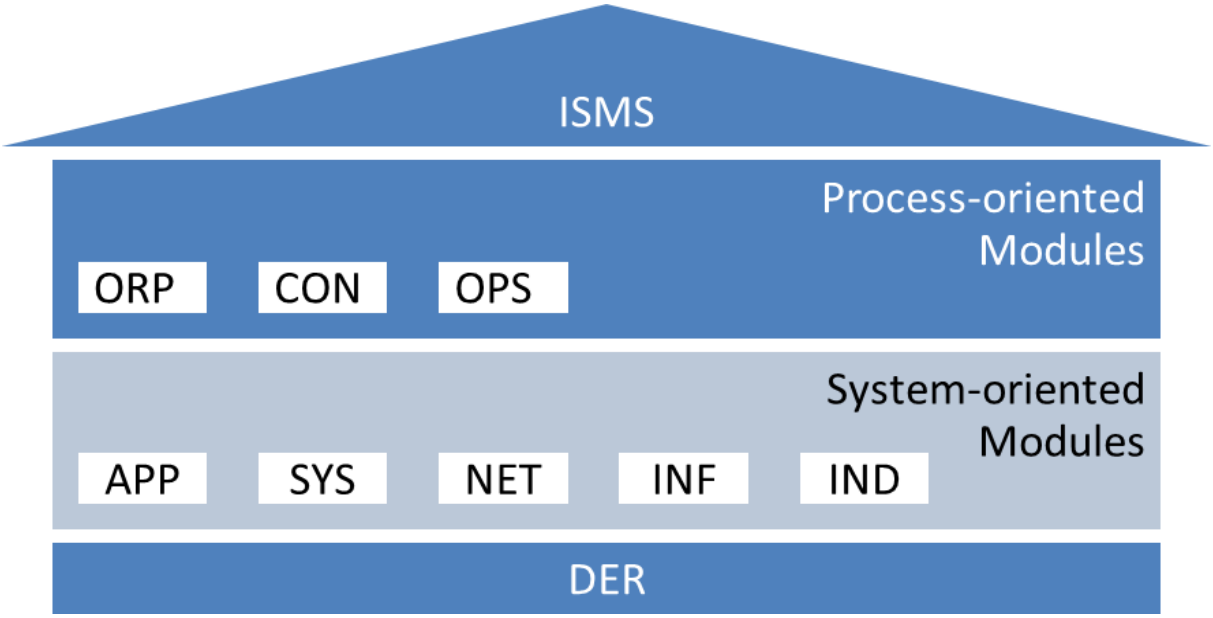


Figure: The layer model of the IT-Grundschutz Compendium

Process modules:

- The ISMS layer contains the module *Security management* as a basis for all subsequent activities in the security process.
- The ORP layer contains the modules covering organisational and personnel security aspects.
- The CON layer contains modules dealing with concepts and approaches.

- The OPS layer comprises all operational security aspects. These are in particular the security aspects concerning the operational side of IT, but also such aspects which should be observed in IT operations for third parties.
- The DER layer contains all modules which are relevant for reviewing the implemented security safeguards and in particular for detecting security incidents and the suitable reactions to those.

System modules:

- The APP layer deals with the safeguarding of applications and services, among other things, in the areas of communication, directory services, network-based services and business and client applications.
- The SYS layer addresses the individual IT systems of the information system that may have been divided into groups.
- The NET layer examines the networking aspects not directly related to specific IT systems, but to the network connections and the communication.
- The INF layer is concerned with architectural and structural factors, in which aspects of the infrastructural security are brought together.
- The IND layer is concerned with security aspects of industrial IT.

The division into process and system modules has the advantage that general aspects and common infrastructural issues can be considered separately from the IT systems. Redundancies are avoided, because individual aspects only need to be addressed once and not for every IT system individually. Breaking down the security aspects into layers also enables individual subject areas within the ensuing security concepts to be updated and expanded more easily, without having a significant effect on other layers.

Order of module implementation

The aim of the IT-Grundschutz Methodology is to enable essential security requirements to be met early and corresponding security safeguards to be implemented. Therefore, the following order is suggested for the implementation of the modules:

- R1: These modules should be implemented as a matter of priority, as they form the basis for an effective security process.
- R2: These modules should be implemented next, as they are required for sustained security in essential parts of the information system.
- R3: These modules are also required in order to achieve the aspired security level and must be implemented, however, it is recommended, to only address them after the other modules.

R1 marks those modules which are required to achieve a basic security framework. These are the following layers:

- ISMS Security management
- ORP Organisation and personnel
- OPS.1.1 Core IT operation

The indicated order is merely a recommendation. Every organisation can define a differing order, as appropriate for their requirements.

Threats

Every module begins with a description of the specific threat scenario for a subject. As an addition, the relevant appendix contains a list of the elementary threats which were considered when creating the module. The list of threads belongs to the first stage of the simplified risk analysis for typical environments of information processing and forms the basis on which the BSI compiled specific requirements, the implementation of which can ensure an appropriate level of information security in an organisation. The advantage is that, for typical scenarios, the users do not need to carry out tedious or additional analyses to achieve the security level needed for normal protection requirements. It is sufficient to identify the modules relevant for the business processes under consideration and their necessary resources and to implement the requirements recommended therein in a consistent and comprehensive manner.

Security requirements

In every module, the security requirements that are relevant for the protection of the object under consideration are listed. They describe what has to be done for its protection. The requirements are grouped into three categories:

- **Basic requirements** must be met as a matter or priority, as with these recommendations maximum benefit can be achieved with (relatively) minimal effort. They are unconditional requirements. The basic requirements form the basis for the Basic Protection approach.
- **Standard requirements** are based on the basic requirements and address normal protection requirements. They should generally be met, but not as a matter of priority. The objectives of the standard requirements must be met to achieve standard safeguarding. However, due to the relevant framework conditions of an organisation, reasons may arise why a standard requirement cannot be implemented as described, but the security objectives are reached in a different manner. If a standard requirement is met by other security safeguards, the arising impacts must be carefully evaluated and documented in an appropriate manner.
- **Requirements for high protection requirements** are a selection of suggestions for extended safeguards that may be considered as a basis for developing suitable requirements and safeguards in case of elevated security requirements or under specific framework conditions.

Implementation recommendations

Detailed implementation recommendations are available for many modules of the IT-Grundschutz Compendium. They describe how the requirements of the modules can be implemented and explain suitable security safeguards with a detailed description. The security safeguards can be used as a basis for security concepts, but should be adapted to the framework conditions of the relevant organisation.

The implementation recommendations address the groups of persons that are responsible for the implementation of the module requirements, for example, the IT operations or building services departments.

5.2 References

[BSI1] Managementsysteme für Informationssicherheit (ISMS) [English version: Information Security Management Systems, BSI Standard 100-1], BSI Standard 200-1, https://www.bsi.bund.de/grundschutz

[BSI2] IT-Grundschutz-Methodik, BSI Standard 200-2 [English version: IT-Grundschutz Methodology, BSI Standard 100-2], https://www.bsi.bund.de/grundschutz

[BSI3] Risikoanalyse auf der Basis von IT-Grundschutz, BSI Standard 200-3 [English version: Risk analysis based on IT-Grundschutz, BSI Standard 100-3], https://www.bsi.bund.de/grundschutz

[GSK] IT-Grundschutz-Kompendium - Standard-Sicherheitsmaßnahmen [English version: IT-Grundschutz Compendium - Standard Security Safeguards], BSI,
new each year, https://www.bsi.bund.de/grundschutz

5.3 Glossary

This glossary lists the most important terms for management systems for information security (ISMS). An additional glossary on cyber security can be found on the BSI website at http://www.bsi.bund.de/cyberglossar.

Assets

Assets refer to inventories of objects which are required for a specific purpose, in particular to meet business objectives. As a synonym for "asset" the term “value” is often used. However, the term “value” can have many meanings – from the social relevance of something up to the internal quality of an object. In the IT-Grundschutz, the term "assets" is used in the meaning of “valuable target objects".

Availability

The availability of services and IT system, IT application, and IT network functions, or even of information is guaranteed if the users are able to use them at all times as intended.

Basic Protection

Basic Protection enables the implementation of comprehensive, basic initial safeguards across all business processes and/or specialist procedures of an organisation as a first entry point into the IT-Grundschutz.

Basic requirement

See Security requirement.

Business process

A business process is a set of logically linked individual activities (tasks, workflows) that are carried out to meet commercial or operational objectives.

Confidentiality

Confidentiality means protection against the unauthorised disclosure of information. Confidential data and information should only be accessible to those authorised using the allowed access methods.

Core Protection

The focus of the cores safeguards is initially on the business processes and assets at particular risk.

Core values of information security

The IT-Grundschutz defines three core values of information security:

- Confidentiality,
- Availability and
- Integrity.

Each user is naturally free to include additional core values when assessing protection requirements if this is helpful in individual cases. Other generic terms concerning information security include, for example:

- Authenticity
- Binding Character

- Reliability
- Non-repudiation

Crown jewels

The term crown jewels refers to such assets the theft, destruction or compromising of which would cause damage threatening the existence of the organisation.

Cyber security

Cyber security is concerned with all aspects of security in information and communication technology. The field of action of information security is extended to the entire cyber space. This comprises all information technology connected to the Internet and comparable networks and includes communication, applications, processes and processed information based on this. A special focus is often on attacks from cyber space when considering cyber security.

Damage / Consequence

A deviation from an expected results leads to a consequence (often referred to as “damage”). As a matter of principle, this can be a positive or a negative deviation.

A positive consequence/positive damage within the meaning of the opportunity and risk analysis is also referred to as an opportunity. In most cases, however, only the negative consequences, I.e. The damage, are considered in the risk analysis.

The scale of a damage is defined as extent of damage and can be referred to as directly quantifiable or not directly quantifiable. The quantifiable damage can usually be described with direct efforts (e.g. of financial nature). Not directly quantifiable damage includes for example damage to one’s image or opportunity costs. In these cases, the actual extent of damage can often only be assumed or estimated. All information is usually classified in categories due to empirical or industry values.

Data protection

Data protection is intended to protect the right to privacy of individuals from being violated through improper handling of his or her personal data. Data protection is therefore used to refer to the protection of personal data against eventual misuse by third parties (not to be confused with the term data security).

The terms "data protection" and "data privacy" differ slightly, though: "Data protection" refers to data protection as a legal concept. The term "data privacy", on the other hand, is more directly related to the lives of people (i.e. the protection of their privacy) and is used primarily in the U.S., although its use is becoming more common in the European Union.

Information security

The aim of information security is to protect information. This information might be stored on paper, on computers, or inside people's heads. IT security primarily concerns protecting and processing information stored electronically. The term “information security” is therefore more comprehensive than the term “IT security” and is being used more and more often. However, since the term “IT security” is still overwhelmingly used in the literature, it will still be used in this and other publications relating to IT-Grundschutz, although the documents will place more and more emphasis on considering information security over time.

Information security management (IS management)

The planning, management, and control roles essential for establishing and continuously implementing a thoroughly thought through and effective process for ensuring information security are referred to as information security management. This is a continuous process to monitor

strategies and concepts on an ongoing basis for their performance and effectiveness and to update them as required.

The term “IT security management” is still frequently used in IT-Grundschutz for the same reasons as mentioned above for the terms “Information security” and “IT security”

Information Security Officer (ISO)

An Information Security Officer (short IS Officer or ISO) is responsible for the operative fulfilment of the task of “information security”. Other designations are CISO (Chief Information Security Officer) or information security manager (ISM). Information security comprises the comprehensive area of the protection of information, namely in and with IT, but also without IT or beyond IT. IT security is thus a subdivision of information security and deals specifically with the protection of the IT employed. In addition to the ISO, there can be a dedicated officer for IT security. This person typically operates in the IT area, while the ISO reports directly to the management level.

Information system

An information system (or also IT system) refers to all infrastructural, organisational, personnel, and technical objects serving to perform tasks in a particular field of application of information processing. An information system may refer to the entire organisation or to individual areas defined by organisational structures (e.g. departments) or joint business processes and/or shared applications (e.g. HR information system).

Information technology (IT)

Information technology (IT) encompasses all technical resources which serve for processing or communicating information. Information processing includes acquisition, recording, use, storage, communication, program-controlled processing, internal display and output of information.

Integrity

Integrity refers to ensuring the correctness (intactness) of data and the correct functioning of systems. When the term integrity is used in connection with the term “data”, it expresses that the data is complete and unchanged. In information technology terms this is, however, used somewhat more widely, also for the term “information”. The term “information” is used for data that, depending on the context, can be associated with certain attributes such as the author or the time and date of creation. Loss of the integrity of information can therefore mean that it was changed without authorisation, the information regarding the author was tampered with or that the date of creation was manipulated.

IT-Grundschutz Check

In IT-Grundschutz, this term refers to the investigation of whether the requirements recommended according to IT-Grundschutz are already met in an organisation and which basic security requirements are still missing (previously: basic security check).

IT-Grundschutz Compendium

The modules of the IT-Grundschutz are summarised in the IT-Grundschutz Compendium. It is the successor to the IT-Grundschutz Catalogues available up to the 15th version.

IT Security Officer

Person with technical competence in IT security who is in charge of aspects around IT security in close cooperation with the IT operation. The role of the person in charge of information security has different names depending on the type and orientation of the organisation. IT-Grundschutz uses the designation Information Security Officer (ISO).

Modules

The IT-Grundschutz Compendium contains explanations regarding the threat scenario, security requirements, and additional information for different processes, components and IT systems, each summarised in a module. The Compendium has a modular structure and its focus is on representing the major security requirements in the modules. According to the basic structure the modules are divided into process- and system-oriented modules, and they are also categorised in a layer model according to subjects.

Organisations

The term “organisations” is used in this context for companies, government agencies, and other public and private organisations.

Policy for information security

The policy is a central document for the information security of an organisation. It describes how information security is to be established in the organisation, for which purposes and with which resources and structures. It contains the information security objectives aimed at by the organisation and the information security strategy pursued. The security policy therefore also describes the level of security aimed at in a government agency or company beyond the security objectives.

Requirements in the case of high protection requirements

See Security requirement.

Risk

Risk is also often defined as the combination (i.e. the product) of the frequency of occurrence of damage and the extent of this damage. The damage is often described as the difference between a planned and unplanned result. Risk is a special form of uncertainty or rather imponderability.

The ISO also defines risk as the result of imponderabilities on target objects. Within this meaning, the term “consequences” is used instead of damage, if events occur differently than expected. In this context, a consequence can be negative (damage) or positive (opportunity). However, the above definition has become more common in practice.

In contrast to the term "threat", the term "risk" includes an assessment of the extent to which a certain damage scenario is relevant to the scenario being examined.

Risk analysis

The term “risk analysis” refers to the complete process for determining (identifying, assessing and evaluating) and treating risks. According to the relevant ISO standards ISO 31000 ISO 27005, “risk analysis” only refers to a single step as part of the risk determination, which consists of the following steps:

- Risk Identification
- Risk Analysis
- Risk Evaluation

In the meantime, however, the term “risk analysis” has been established for the entire process of risk determination and risk treatment. Therefore, the term “risk analysis” is still used in this document to refer to the comprehensive process.

Risk management

Risk management refers to all activities with respect to the strategic and operative treatment of risks, i.e. all activities to identify, control and monitor risks for an organisation.

The strategic risk management describes the essential framework conditions how the handling of risks within an organisation, the culture regarding the handling of risks and the methodology are designed. These principles for the treatment risks within an ISMS must be consistent with the framework conditions of the organisation-wide risk management or coordinated.

The framework conditions of the operative risk management include the control process consisting of

- Risk identification
- Risk assessment and evaluation
- Risk treatment
- Risk monitoring and
- risk communication

Security concept

A security concept serves to implement the security strategy and describes the approach planned to achieve the security objectives set in an organisation. The security concept is the main document in the security process of a company and/or government agency. It must be possible to trace every security safeguard back to the security concept.

Security design

The creation of a security design is one of the primary tasks of information security management. Based on the results of the structure analysis and the protection requirements determination, the required security safeguards are identified and documented in the security concept.

Security policy

In a security policy the security objectives and general security requirements are formulated in the sense of the official regulations of a company or a government agency. Detailed security safeguards are contained in a more comprehensive security concept.

Security requirement

The term “security requirement” refers to requirements for the organisational, personal, infrastructural and technical area the fulfilment of which is necessary in order to increase the information security or contributes towards it. A security requirements also describes what has to be done in order to achieve a specific level regarding the information security. How the requirements can be fulfilled in the specific case is described in corresponding security safeguards (see there). The term "control" is also often used for security requirements.

The IT-Grundschutz differentiates between basic safeguards, standard safeguards and requirements in the case of high protection requirements. Basic requirements are fundamental and must always be implemented, unless there are substantial reasons against it. Standard requirements must generally be implemented for normal requirements, unless they are replaced by at least equal alternatives or the deliberate acceptance of the residual risk. Requirements in the case of high protection requirements are exemplary suggestions, which should be implemented in an appropriate manner in the case of corresponding protection requirements.

Security safeguard

The term security safeguard (safeguard for short) refers to all actions serving to control and counteract security risks. This includes organisational, personnel, technical or infrastructural security safeguards. Security safeguards serve to fulfil security requirements (see there). The terms security precaution and protective measure are often used synonymously. "Security measure” or “measure” are also used.

Specialised task

Specialised tasks are tasks resulting from an organisation's specific purpose or mission. In the IT-Grundschutz, the term "specialise tasks" is used for business processes in government agencies.

Standard Protection

Standard Protection essentially corresponds to the classic IT-Grundschutz Methodology. Standard Protection provides an ISO with the means for comprehensive and in-depth safeguarding of the assets and processes of an organisation.

Standard requirement

See Security requirement.

Structure analysis

As part of a structure analysis, the necessary information on the selected information system, applications, IT systems, networks, rooms, buildings, and connections is captured and prepared in such a way that it supports the next steps of IT-Grundschutz.

Target objects

Target objects are those parts of the information system one or several modules from the IT-Grundschutz Compendium can be assigned to within the framework of modelling. Target objects may include physical objects, such as networks or IT systems. Often however, target objects are logical objects such as organisational units, applications, or the entire information system.

Threat

A threat is a basic threat with a direct effect on an object as the result of a vulnerability. A threat therefore only becomes an imminent threat for an object when it is combined with a vulnerability.

For example, is harmful software a basic or applied threat to the user who is surfing the Internet? According to the above definition it can be ascertained that all users are principally exposed to a basic threat by harmful software on the Internet. The user who downloads an infected file is exposed to a threat by the harmful software, if his computer is vulnerable to this type of harmful software. Users with effective anti-virus protection, a configuration preventing the harmful software from working, or an operating system not able to execute the code of the harmful software are not exposed to a threat as a result of the downloaded harmful software, however.

Vulnerability

A vulnerability is a security-relevant error of an IT systems of an organisation. Causes may include the design, the algorithms used, the implementation, the configuration, or the operation, as well as the organisation itself. A vulnerability may cause a threat to become effective and damage an organisation or a system. As a result of a vulnerability an object (an organisation or a system) is susceptible to threats.