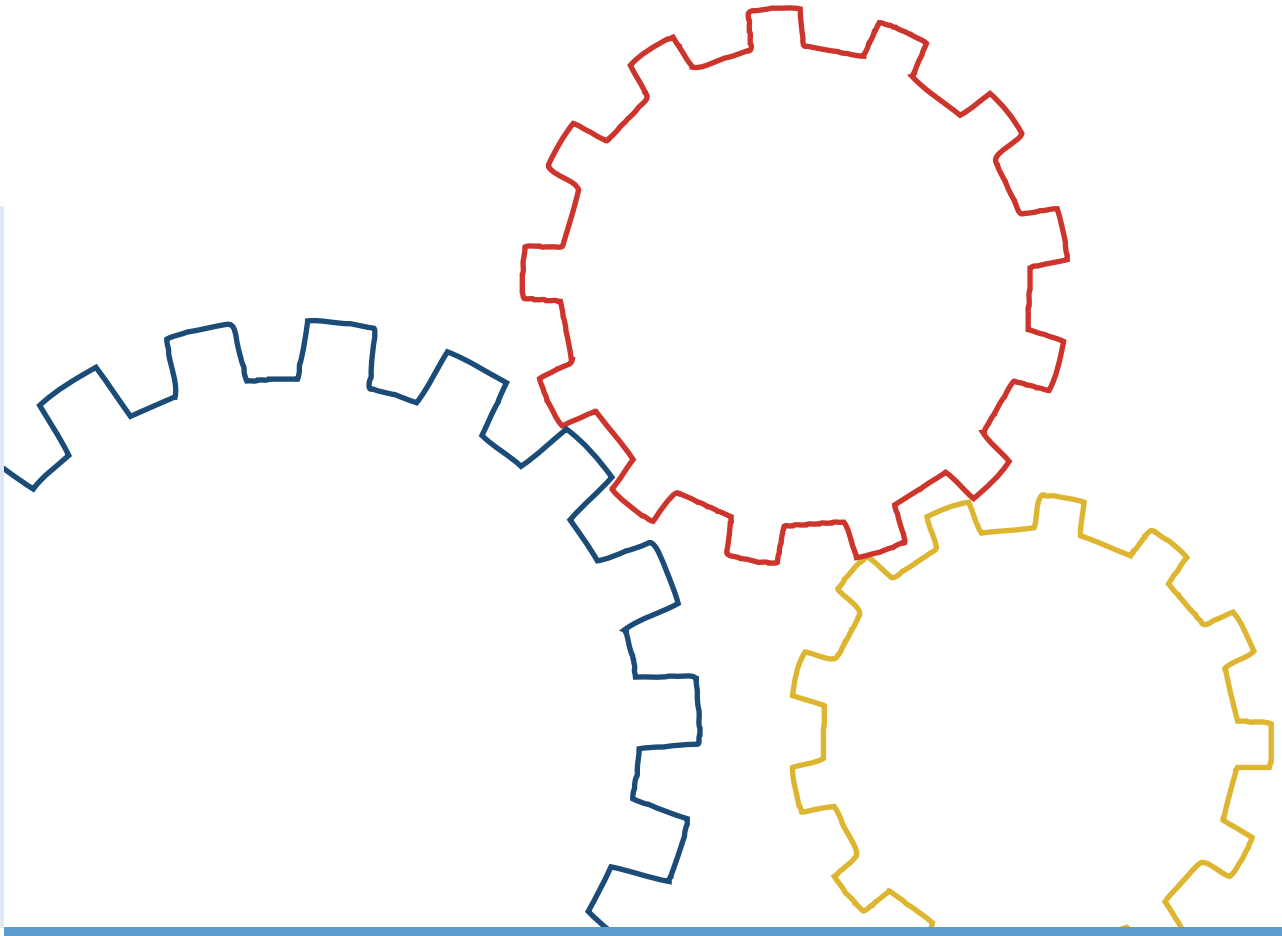
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 100-2

IT-Grundschutz Methodology



www.bsi.bund.de/grundschutz

Version 2.0

Contents

1 Introduction

1.1 Version History

As per	Version	Changes
December 2005	1.0	
May 2008	2.0	▪ Stronger emphasis on the information security instead of the IT security, resulting in the modification of various terms ▪ Addition of data protection aspects ▪ Updated to reflect new and revised ISO standards ▪ Improved organisation ▪ The order of the categories in the structure analysis has been changed. ▪ Clearer separation of the tasks in the security process both in the preparatory tasks in Chapter 3 and in the implementation in Chapters 4 to 6

1.2 Objective

The IT-Grundschutz Methodology is a BSI methodology for effective management of the information security that can be easily adapted to the situation of a specific organization.

The procedure described in the following chapters is based on the BSI Standard 100-1 "Management Systems for Information Security (ISMS)" (refer to [BSI1]) and explains the IT-Grundschutz Methodology presented in BSI Standard 100-1. A management system for information security (ISMS) is the planned and organised course of action taken to achieve and maintain an appropriate level of information security. For this reason, the suggested implementation for IT-Grundschutz is presented explicitly for every single phase described in BSI Standard 100-1.

IT-Grundschutz represents a standard for establishing and maintaining an appropriate level of protection for all information at an organisation. This method, which was introduced by BSI in 1994 and has been refined and developed ever since then, provides both a methodology for setting up a management system for information security and a comprehensive basis for assessing risks, monitoring the existing security level, and implementing the appropriate information safeguards.

One of the most important objectives of IT-Grundschutz is to reduce the expense of the information security process by offering reusable bundles of familiar procedures to improve information security. In this manner, the IT-Grundschutz Catalogues contain standard threats and security safeguards for typical business processes and IT systems which can be used in your organisation, if necessary. Through appropriate application of the standard technical, organisational, personnel, and infrastructural security safeguards recommended for IT-Grundschutz, a security level is reached for the business processes being analysed that is appropriate and adequate to protect business-related information having normal protection requirements. Furthermore, the safeguards in the IT-Grundschutz Catalogues not only form a basis for IT systems and applications requiring a high level of protection, but also provide an even higher level of security in many areas.

1.3 Target group

This document is primarily aimed at those who are responsible for security, security officers, security experts, security consultants, and anyone interested who is familiar with the information security management. It also provides a practical foundation for those responsible for IT, the management personnel, and the project managers who ensure that the security issues in their projects or organisation have been adequately taken into account.

The IT-Grundschutz Methodology is aimed at organisations of all types and sizes that require a cost-effective and targeted method of setting up and implementing the appropriate level of security in their organisation. The term "organisation" is used in this context for companies, government agencies, and other public and private organisations. IT-Grundschutz can be implemented by small organisations as well as in large organisations. Note, though, that all recommendations should be examined and appropriately implemented in the context of the particular organisation.

1.4 Application

BSI Standard 100-1 "Management Systems for Information Security" describes the general methods for the initiation and management of information security in an organisation. The IT-Grundschutz Methodology now provides specific assistance on how to introduce a management system for information security step by step. IT also discusses the individual phases of this process and presents practical, model solutions, so-called "best practice" approaches, to accomplish the tasks.

This methodology provides a comprehensive framework for an ISMS and only needs to be adapted to the individual conditions in an organisation so a suitable management system for information security can be set up. In order to successfully establish a continuous and effective information security process, an entire series of actions must be performed. The IT-Grundschutz Methodology and the IT-Grundschutz Catalogues provide information on the methodology and practical aids for its implementation.

Furthermore, the IT-Grundschutz Methodology also provides a standard with which an organisation can publicise the quality of its own ISMS via a certificate and which can be used as a criterion to assess the level of maturity of the ISMS in other organisations.

ISO 27001 certification based on IT-Grundschutz can also be used as a security requirement for potential co-operation partners in order to define the required level of information security in the partner's organisation. Even if a different methodology is used as the basis for the ISMS, it is still possible to benefit from the IT-Grundschutz Methodology. For example, IT-Grundschutz also provides approaches to solutions for various issues relating to information security, for example for the creation of concepts, performing audits, and for certification in the area of the information security. Depending on the task at hand, different ways of applying IT-Grundschutz may be appropriate, for example by applying only some aspects of it. Depending on the area of application, individual modules, the threat and safeguard catalogues, and other aids provided by IT-Grundschutz form a helpful basis for security management tasks.

Chapter 2 provides a summary of the most importance steps for introducing an ISMS and the procedure to follow to produce a security concept.

Chapter 3 describes how the fundamental phase in initiating the information security process could look and which organisational structures are appropriate for the process. In addition, a systematic path is shown for setting up a functioning security management system and for developing it further during live operation.

Chapter 4 describes the IT-Grundschutz Methodology used to produce a security concept. This chapter first shows how the basic information on an information domain can be collected and reduced by forming groups. Subsequently, the protection requirements for the applications, IT systems, communication links, and rooms must be determined based on the business processes. The

appropriate modules and safeguards from the recommendations in the IT-Grundschutz Catalogues must then be selected for the relevant information domain, i.e. they are modelled in accordance with IT-Grundschutz Methodology. Before implementing the security safeguards, the existing and additional security safeguards which were, for example, defined and detected in the supplemental security analysis and in the subsequent risk analysis based on IT-Grundschutz according to BSI Standard 100-3 (refer to [BSI3]) must be integrated into the IT-Grundschutz Methodology.

Chapter 5 then describes how the detected and consolidated security safeguards should subsequently be implemented.

The main task of an ISMS is to ensure that information security is maintained. This subject is tackled in Chapter 6, and the possibility of publicising the security level attained in the form of a certificate is presented as well.

The IT-Grundschutz Methodology, and in particular the IT-Grundschutz Catalogues, are expanded and adapted to reflect recent developments regularly. Due to the constant exchange of information with the users of IT-Grundschutz, it is possible to continually development the catalogues to reflect new requirements. The ultimate objective of these efforts, though, is to point out the current recommendations for common security problems.

1.5 References

[BSI1] Information Security Management Systems (ISMS), BSI Standard 100-1, Version 1.5, May 2008, www.bsi.bund.de

[BSI2] IT-Grundschutz Methodology, BSI Standard 100-2, Version 2.0, May 2008, www.bsi.bund.de

[BSI3] Risk Analysis on the Basis of IT-Grundschutz, BSI Standard 100-3, Version 2.5, May 2008, www.bsi.bund.de

[GSK] IT-Grundschutz Catalogues – Standard Security Safeguards, BSI, new each year, http://www.bsi.bund.de/grundschutz

[SHB] IT Security Manual – Manual for the secure application of information technology, BSI, Version 1.0 – March 1992, Bundesdruckerei

[OECD] Organisation for Economic Co-operation and Development (OECD), Guidelines for the Security of Information Systems and Networks, 2002, www.oecd.org/sti/security-privacy

[ZERT] Certification according to ISO 27001 on the basis of IT-Grundschutz - audit scheme for ISO 27001 audits, BSI, Version 1.2, March 2008, www.bsi.bund.de/grundschutz/zert

[ZERT2] Certification scheme for audit team leaders for ISO 27001 audits on the basis of IT-Grundschutz, BSI, Version 1.2, March 2008, www.bsi.bund.de/grundschutz/zert

[27000] ISO/IEC 27000 (3rd CD, 2008) "ISMS – Overview and Vocabulary", ISO/IEC JTC1/SC27

[27001] ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems requirements specification", ISO/IEC JTC1/SC27

[27002] ISO/IEC 27002:2005 "Information technology - Code of practice for information security management", ISO/IEC JTC1/SC27

[27005] ISO/IEC 27005 (2nd FCD, 2008) "Information security risk management", ISO/IEC JTC1/SC27

2 Information security management with IT-Grundschutz

Information is highly valuable to companies and government offices and needs to be appropriately protected. Most information today is created, stored, transported, or processed at least in part using information technology (IT). It is impossible to imagine modern business processes without IT support in companies and administration offices. A reliable system for processing information is essential to be able to maintain operations in an organisation. Inadequately protected information is a frequently underestimated risk factor that can threaten the existence of some organisations. However, reasonable information protection as well as baseline protection for the IT systems can be achieved with relatively modest resources.

Note, though, that it takes more than simply purchasing anti-virus software, firewalls, or data back-up systems to achieve a level of security for all business processes, information, and IT systems in an organisation that meets the requirements. It is important to take a holistic approach. This includes, above all, a functional security management that is integrated into the organisation. Information security management (or IS management for short) is the part of general risk management intended to ensure the confidentiality, integrity, and availability of information, applications and IT systems. This process is a continuous process whose strategies and concepts are monitored on an ongoing basis for their performance and effectiveness and adapted when necessary.

Information security is not only a question of technology, but depends a great deal on the general organisational and personnel requirements. The BSI IT-Grundschutz Methodology and the IT-Grundschutz Catalogues have taken this into account for a long time already by recommending both technical and non-technical standard security safeguards for common business areas, applications, and IT systems. In this context, emphasis is placed on practical and action-based information with the goal of keeping the entry barriers of the security process as low as possible and avoiding highly complex procedures.

The IT-Grundschutz Methodology describes how an efficient management system for information security can be set up and how the IT-Grundschutz Catalogues can be used for this purpose. The IT-Grundschutz Methodology combined with the IT-Grundschutz Catalogues provide a systematic method for developing security concepts and practical, standard security safeguards that have already been successfully implemented by numerous government agencies and companies.

The IT-Grundschutz Catalogues, which were published the first time in 1994 and now contain over 4000 pages, describe potential threats and protective safeguards in detail. The IT-Grundschutz Catalogues are constantly being revised, and new, specialised subjects are added as required. All information on IT-Grundschutz is available free of charge from the BSI website. In order to support the international co-operation of government agencies and companies, all documents relating to IT-Grundschutz are also available in English and in electronic form.

More and more business processes are being linked together via information and communication technology. This is accompanied by increases in the complexity of the technical systems and with a growing dependence on the correct operation of the technology. For this reason, all those involved must be plan and organise the procedures in order to implement and maintain an appropriate level of security. The only way to guarantee that this process will be anchored in all business areas is by making it a high priority task in the top management level. The highest level of management is responsible for the correct and targeted operation of an organisation, and hence for guaranteeing information security internally and externally. They are thus responsible for initiating, controlling, and monitoring the security process. This includes issuing key strategic statements on information security, conceptual requirements, and the organisational framework to be used to attain information security in all business processes.

The responsibility for information security remains at this level in any case, but the task of ensuring "information security" is usually delegated to an information security officer. In the IT-Grundschutz documents, this role is often referred to as the “IT Security Officer” even when the job of an IT Security Officer extends beyond pure IT security tasks.

If this framework does not exist in a given situation, then the first step should be an attempt to implement the missing security safeguards into the daily routine. In all cases, though, the idea is to raise the awareness of management for information security issues so that they will bear their share of the responsibility for information security in the future. Although many aspects of the information security process can even be initiated in daily operations and will result in an improvement in the security situation; there is no guarantee that such actions will lead to a permanent increase in the level of information security.

The IT-Grundschutz Methodology describes a method for setting up and integrating IS management in an organisation. If an organisation has effective IS management integrated into the business processes, it can be assumed that it is in a position to achieve the desired security level, to improve it where necessary, but that it will be able to meet new challenges as well.

A consolidated, properly functioning security management is the essential basis for the reliable and continuous implementation of security safeguards in an organisation. For this reason, there is also a *Security Management* module in the IT-Grundschutz Catalogues in addition to the detailed information available in this document. This module is used to achieve a uniform method of applying IT-Grundschutz and for integrating security management in the certification process in accordance with IT-Grundschutz to the extent it should be accorded due to its importance.

In addition to the IT-Grundschutz Methodology, the IT-Grundschutz Catalogues also provide implementation aids for the security process in the form of field-proven, standard security safeguards. IT-Grundschutz uses a holistic approach to this process. Through appropriate application of the standard technical, organisational, personnel, and infrastructural security safeguards, a security level is reached that is appropriate and adequate to protect business-related information having normal protection requirements. Furthermore, these safeguards not only form a basis for IT systems and applications requiring a high level of protection, but also provides an even higher level of security in many areas.

The IT-Grundschutz Catalogues describe how to create and monitor security concepts based on standard security safeguards. Suitable bundles ("modules") of standard security safeguards are available for common processes, applications, and components used in information technology. These modules are classified into five different layers according to their focus:

- Layer 1 covers all generic information security issues. These include the human resources, data backup concept, and outsourcing modules.
- Layer 2 covers the technical issues related to building construction. Examples include the modules for buildings, server rooms, and home offices.
- Layer 3 covers individual IT systems. Examples include the general client, general server, telecommunication system, laptop, and mobile telephone modules.
- Layer 4 concerns the issues relating to networking IT systems. Examples include the heterogeneous networks, WLAN, VoIP, network management, and system management modules
- Finally, Layer 5 deals with the actual applications. Examples include the e-mail, web server, and database modules

Each module contains a brief description of the issue, a list of references to the relevant threats, and a list of references to the corresponding standard security safeguards. The threats and safeguards are in turn distributed individually among the threat and safeguard catalogues. The threats are classified into the force majeure, organisational defects, human error, technical failure, and deliberate acts categories. The safeguards are grouped in the infrastructure, organisation, personnel, hardware and software, and communication and contingency planning catalogues.

2.1 Scope of the subject areas

The goal of information security is to protect information. This information may be stored on paper, in computers, or in the knowledge of the employees. IT security primarily concerns protecting and processing information which is stored electronically. The term "information security" is therefore more comprehensive than the term “IT security” and is being used more and more often. IT-Grundschutz has followed a holistic approach for a long time already. This approach also protects business-related information and business processes that are not supported or only supported in part by IT systems. However, since the term "IT security" is still overwhelmingly used in the literature, we will continue to use this term in this and other publications relating to IT-Grundschutz, although the documents will place more and more emphasis over time on examining information security.

The job of information security is to provide appropriate protection for the basic values of confidentiality, integrity (correctness), and availability of information. This also includes securing the processing of information, i.e. the IT in particular. In addition, this also includes the authenticity and undeniability of information and messages as special cases of information integrity.

The planning and management role essential to setting up and continuously implementing a well thought-out and effective process for establishing information security is referred to as information security management. The term "IT security management" is still used often in many BSI documents instead of the term “information security management" (or its abbreviated form, IS management) for the same reasons as stated above for the terms "information security" and "IT security".

2.2 Overview of the information security process

The IT-Grundschutz Methodology provides assistance in setting up and maintaining the information security process in an organisation by revealing paths and methods for the general course of action, but also for solutions to special problems.

In order to achieve an appropriate level of security, a systematic approach is required to design the security process. The security process is comprised of the following phases in the context of IT-Grundschutz:

- Initiation of the security process
  - Accepting of responsibility by the management
  - Designing and planning the security process
  - Creation of the policy for information security
  - Establishment of a suitable organisational structure for information security management
  - Provision of financial resources, personnel, and the necessary time
  - Integration of all employees in the security process
  - Creation of a security concept
  - Implementation of the security concept
  - Maintenance of information security during live operations and implementation of a continuous improvement process

Those responsible for information security can use the IT-Grundschutz Methodology and IT-Grundschutz Catalogues to set goals and for various other reasons. Accordingly, the order of implementation and intensity of the individual phases depends on the existing security environment and the perspectives of the corresponding users. For example, emphasis is often placed on different aspects when performing a regular update of the security concept than when integrating new business processes.

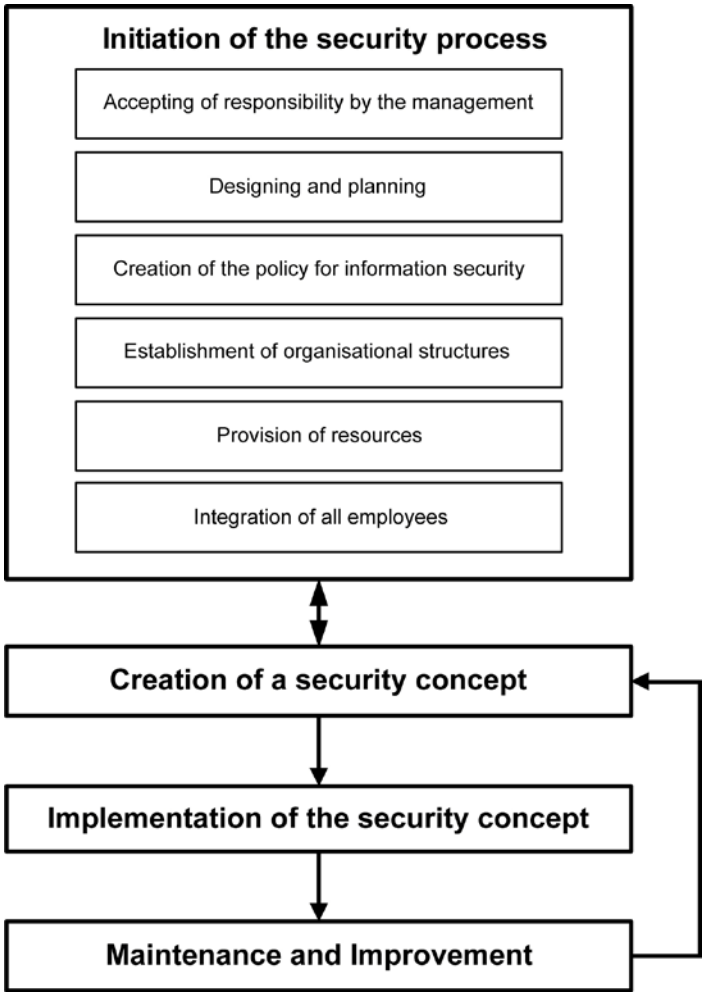


Figure 1: Phases of the security process

Some of these phases can be implemented in parallel, meaning the design and planning phases of the security process can be performed at the same time as the information security organisation is established. The training and raising of awareness can be done at any time throughout the whole process. In this case, the advance phases must be updated quickly to take the new results into account.

The following provides a short description of the phases involved in the security process.

Initiation of the security process

The management must initiate, control, and monitor the security process. To accomplish this, key strategic statements on information security as well as the organisational framework are required. Chapter 3 describes how to set up a functioning security process and which organisational structures are needed for this purpose.

Creation of a security concept

A number of steps are involved in the creation of a security concept for IT-Grundschutz, and these steps are described in detail in Chapter 4. The main steps are:

- Structure analysis
- Determination of the protection requirements
- Selection and adaptation of safeguards
- Basic security check
- Supplementary security analysis

Implementing security concepts

A satisfactory level of security can only be attained if the existing vulnerabilities are determined in the security analysis, the status quo is recorded in a security concept, the necessary safeguards have been identified and, above all, these safeguards are also thoroughly implemented. Chapter 5 describes what you need to consider when planning the implementation of security safeguards.

Maintenance and continuous improvement of the information security

The goal of security management is to attain the desired level of security, maintain this level over the long term, and improve the level of security. For this reason, the appropriateness, effectiveness, and efficiency of the security process and the organisational structures for information security must be checked regularly. It must also be examined if the **safeguards** in the **security concept** are practical and if they have been implemented correctly. In Chapter 6, the actions which should be taken to maintain and improve information security are presented in the form of an overview.

ISO 27001 certification on the basis of IT-Grundschutz

The IT-Grundschutz Methodology and the IT-Grundschutz Catalogues are not only used in the security concept, but are also being used more and more as reference, i.e. as a security standard. Through IT-Grundschutz certification based on ISO 27001 based on IT-Grundschutz, an organisation can document internally and externally that they have implemented ISO 27001 as well as IT-Grundschutz to the proper extent. Chapter 7 provides a short survey of the steps to take to achieve this and which conditions must be fulfilled for successful certification.

2.3 Application of the IT-Grundschutz Catalogues

After the management has defined the policy for information security and the design of the information security organisation in the strategic level, the policy is pursued in the operative level with the help of the **security concept**. The creation of a security concept is therefore one of the primary tasks of information security management. Building on the results on the previous phase, the required security safeguards are now identified and documented in the security concept.

In order to better prepare and organise the highly heterogeneous areas of the IT including the application environment, IT-Grundschutz follows a modular principle. The individual modules described in the IT-Grundschutz Catalogues reflect typical areas and aspects of information security in an organisation ranging from generic issues such as IS management, contingency planning, the data backup concept, and through to the special components in an IT environment. The IT-Grundschutz Catalogues cover the threat scenarios and the recommended safeguards for various components, procedures, and IT systems, which are then consolidated into one module for each subject. The BSI revises and updates the existing modules at regular intervals so that the recommendations reflect the most recent developments in technology. In addition, new modules are regularly added to the existing body of documentation.

The modules play a central role in the IT-Grundschutz Methodology. The modules all have the same layout in order to simplify their use. Each module starts with a short description of the components, approach, or IT system under review. The threat scenarios are then described. The threats are classified into the areas of force majeure, organisational defects, human error, technical failure, and deliberate acts.

The safeguards listed in the IT-Grundschutz Catalogues are standard security safeguards, i.e. they are safeguards to be implemented for the corresponding module according to the current state of technology in order to achieve an appropriate basic level of security. In this context, the safeguards required for ISO 27001 certification based on IT-Grundschutz represent the minimum of security precautions to be implemented to achieve a reasonable level of baseline protection in any case. These **safeguards** are labelled in the IT-Grundschutz Catalogues using the letters A, B, and C. The safeguards marked as "additional" have also been proven in practical applications, but they are aimed

at applications with higher protection requirements. Furthermore, there are also safeguards labelled with a "K" that serve to transfer knowledge.

Security concepts that have been produced with the aid of IT-Grundschutz are compact because in the concept, you only need to refer to the relevant safeguards in the IT-Grundschutz Catalogues. This makes them clearer and easier to understand. To be able to implement the recommended security safeguards more easily, the safeguards are described in detail in catalogues. Note that when we use specialised terminology, we made sure the descriptions will be understood by those who have to implement the safeguards.

To simplify the implementation of the safeguards, the text from the IT-Grundschutz Catalogues is also available in full in electronic form. In addition, support is also provided for the implementation of the safeguards using auxiliary materials and sample solutions, which have been provided in part by the BSI and in part by IT-Grundschutz users.

Additional information can be found in the introductory sections of the IT-Grundschutz Catalogues and in section 4.4 of this **standard**.

3 Initiation of the security process

To achieve and maintain an appropriate and adequate level of information security in an organisation, a planned approach is required as well as an adequate organisational structure. It is also necessary to define security objectives and a strategy for achieving these objectives as well as for setting up a continuous security process. Because of the importance and far-reaching consequences of the decisions to be made and the responsibility for these decisions, this process must be initiated by the highest level of management.

3.1 Accepting Responsibility by Management

The top management level of every **government agency and every company** is responsible for **the proper functioning of all business areas, for ensuring the business processes are on target, and for detecting and minimising risks in time**. Depending on the type of organisation and business area, this may also be regulated by various laws. As the dependency of the business processes on information technology increases, the requirements for ensuring internal and external information security also increase.

The management must initiate, control, and monitor the security process. The responsibility for information security remains at this level, but the job of achieving and maintaining "information security" is usually delegated to an IT Security Officer. In the process, the management must be intensively involved in the "information security management process". This is the only way the information security management can ensure that there are no unacceptable risks remaining and that resources are invested in the right locations. Top-level management is therefore the entity required to make decisions on how to handle risks and to provide the corresponding resources.

The fact that management bears the responsibility for preventing and handling security risks is often not realised in time by the management. Accordingly, the authorities and responsibilities for information security issues are frequently left unresolved. After a security incident occurs, the timely provision of information on potential risks when handling information, business processes, and IT systems is often considered by management or the head of a government agency to be the responsibility of the IT or security experts. For this reason, it is recommended that the experts inform the management about the potential risks and consequences of a lack of information security. In any case, though, management is still responsible for ensuring that they receive the required scope of information in time. Issues relating to security include, for example:

- The security risks for the organisation and its information, including an indication of the effects and costs associated with these risks.
- The effects of security incidents on the critical business processes should be illustrated.
- The security requirements resulting from legal and contractual stipulations must be described.
- The typical, standard approaches to information security for the industry should be presented.
- The advantages of certification, i.e. the ability to demonstrate the level of information security attained to customers, business partners, and supervisory organisations, should be explained.

Since statements made by uninvolved third parties are often given more weight than the statements from one's own staff, it is advisable to use external consultants to raise awareness of information security with the management or heads of a government agency.

Although management is responsible for achieving the security objectives, all employees in an organisation must support the security process and help design it. Ideally, the following principles should be followed:

- The initiative for information security should originate in the management level of the company or government agency.

- The top management level is responsible in general for information security.
- The "information security" function should be actively supported by the government agency or company management.
- The agency administration or company management appoints the employees responsible for information security and provides them with the necessary authorities and resources.
- The management level acts as a role model when it comes to information security. This means that management must also follow all security rules specified, among other things.

Above all, the management must ensure that information security is integrated into all relevant business processes, specialised procedures, and projects. Experience has shown that, due to the omnipresent pressure to succeed, the IT Security Officer requires the full support of management to be included in all key activities by the persons responsible for the corresponding specialised areas.

Management must set the objectives both for information security management and all other areas so that the desired security level can be reached in all areas with the resources (personnel, time, financial) provided.

Action Points for 3.1 Accepting Responsibility by Management
▪ The management is informed about the possible risks and consequences of insufficient information security.
▪ The management assumes full responsibility for information security.
▪ The management initiates the information security process within the **organisation**.

3.2 Designing and planning the security process

In order to achieve and maintain an appropriate level of security, a continuous information security process must be established, and an appropriate information security strategy (IS strategy) must be specified. An IS strategy is used to plan how to proceed in the future in order to achieve the specified security objectives. Management specifies the strategy, which is based on the company's business objectives or the government agency's role. Management specifies the basic security objectives and the level of information security appropriate for the business objectives or specialised tasks. Management must also provide the resources necessary to accomplish this.

3.2.1 Determining the Environmental Conditions

The fundamental objectives and mission of an organisation are the basis for all business processes and specialised procedures and activities, including information security. In order to specify an appropriate IS strategy, every organisation must determine which business processes and specialised tasks are most important as well as their information security requirements. Nowadays, there are hardly any central business processes that can operate without the support of IT. The **decision of which security level** is appropriate to protect the information and the information technology is based on the relationship between the business processes and the information they process as well as the information technology used. This decision-making process is described in greater detail in the following.

A contact person must be appointed for every business process and specialised task who acts as the so-called "information owner" for all questions relating to information processing data in the context of the given business process. The specialist or information owner is responsible, for example, for delegating tasks and handling information in the business processes they have been assigned to manage. It must be specified how critical the information handled is for every business process and specialised task, i.e. the level of protection required must be specified. Finally, management must agree to the protection requirements specified for each business process because the security requirements are derived from these and the corresponding resources will need to be provided.

The analysis of the business processes provides information on the effects of security incidents on the business activities. In many cases, it is adequate to work with a very rough description of the business processes.

The following questions should be answered:

- Which business processes are present in the organisation and how are they related to the business objectives?
- Which business processes depend on a functioning information technology infrastructure, i.e. on IT that meets the requirements and operates properly?
- Which information is processed for these business processes?
- Which information is particularly important and therefore worthy of protection in terms of confidentiality, integrity, and availability and why is it important (e.g. personal data, customer data, strategic information, secrets such as development plans, patents, procedure descriptions)?

A variety of internal conditions can affect information security, and these conditions must be determined. In this early stage, it is not important to describe the information technology in detail. However, there should be a basic overview available of which information is processed for a business process with which applications and IT systems.

In addition, all external conditions that could have and effect on the information security must be determined. These conditions could include, for example:

- legal requirements (national and international laws and regulation),
- environmental factors, for example due to the geographic location or the underlying social and cultural context,
- requirements from customers, suppliers, and business partners, the current market conditions, competitors, and other market-related dependencies, and
- industry-specific security standards.

In order to determine all relevant conditions for every key business process as quickly and with as much detail as possible, it is recommended to hold a brief security meeting (brainstorming session) for each business process. The security meetings should be led by the IT Security Officer, and the relevant information owner or specialist responsible as well as the person responsible for IT should also be present. The results should be documented in a form specified beforehand for this purpose.

3.2.2 Formulation of general information security objectives

The information security objectives should be determined carefully at the start of every security process. Otherwise, there is a risk that the security strategies and concepts worked out will not meet the actual requirements of the organisation. In this case, the result may be that the organisation takes unwanted risks or invests too much in inappropriate or overly complex security safeguards.

For this reason, general security objects should be derived first from the organisation's basic objectives and the general requirements. Specific security requirements for handling information and for IT operations are derived from these later when producing the security concept and designing the information security organisation. Potential general security objectives for an organisation may include, for example:

- High handling reliability, also in terms of handling information (availability, integrity, confidentiality)
- Insuring the good reputation of the organisation in the general public,
- Preserving the value of investments in technology, information, work processes, and knowledge,
- Protecting the high and possibly irreplaceable value of the process information,

- Protecting the quality of information, for example when it serves as the basis for decisions with broad consequences,
- Ensuring the requirements resulting from legal regulations are met,
- Reducing the costs incurred when a security incident occurs (by both avoiding and preventing damage), and
- Ensuring the continuity of the work processes in the organisation.

In order to be able to define the security objectives, the organisation must assess which business processes, specialised procedures, and information are essential to meet the objectives and how valuable they are. It is important during the assessment to clarify how strongly the fulfilment of the organisation's objectives depends on the confidentiality, integrity, and availability of the information needed and on the secure operation of the IT used. In order to define the security objectives, it is advisable to expressly state the basic protection values of availability, integrity, and confidentiality, and possibly assign priorities to them. These statements play a decisive role in the course of the security process when selecting the security safeguards and strategies.

However, determining the information security objectives and the desired level of security is just the beginning of the information security process. Specific decisions on resources and investments that arise during the security process also need to be approved by top-level management in a later phase. This means that no detailed analyses of the information domain and of the potential cost of security safeguards are required at this point. All that is required is a statement of what is especially important to the organisation and why.

3.2.3 Determining the appropriate security level for the business process

In order to better understand the information security objectives, the desired security level for individual business processes or organisational areas of particular interest can be described in terms of the basic components of information security (confidentiality, integrity, availability). This is useful later when specifying the detailed security concept.

The following lists some examples of the criteria used to determine an appropriate level of security. The security level (normal, high, or very high) can be determined according to which statements are the most applicable to the situation. This phase of the security process deals with formulating an initial set of general statements that will then be used as the foundation for later phases, and not with determining the protection requirements in detail.

Very high:

- The protection of confidential information must be guaranteed and comply with strict confidentiality requirements in areas critical to security.
- It is essential that the information is correct.
- The primary tasks of the organisation cannot be performed without IT. Swift reaction times for critical decisions require the constant presence of up-to-date information; downtimes are unacceptable.
- The protection of personal data absolutely must be guaranteed. Otherwise, there may be a risk of injury or death to the persons involved, or the personal freedom of the persons involved could be endangered.

The following generally applies: failure of the IT leads to the total collapse of the organisation or has serious consequences for large parts of society or the economy.

High:

- The protection of confidential information must meet high requirements, and must be even stronger in areas critical to security.

- The information processed must be correct; errors must be detectable and avoidable.
- There are time-critical procedures or a multitude of tasks are performed in central areas of the organisation that could not be performed without the use of IT. Only very short downtimes can be tolerated.
- The protection of personal data must meet high requirements. Otherwise, there is a risk that the social standing or financial well-being of those concerned could be seriously affected.

The following generally applies: in the event of damage, key areas of the organisation can no longer function; the damage leads to significant impairment of the organisation itself or of affected third parties.

Normal:

- The protection of information only intended for internal use must be guaranteed.
- Minor errors can be tolerated. Errors that significantly affect the ability to perform the tasks must be detectable or avoidable.
- Extended downtimes leading to missed deadlines cannot be tolerated
- The protection of personal data must be guaranteed. Otherwise, there is a risk that the social standing or financial well-being of those concerned could be adversely affected.

The following generally applies: damage leads to the impairment of the organisation.

The involvement of management when specifying the information security objectives is essential. For this step, which is essential to the security process, it may be appropriate to consult an external information security expert. To determine the desired level of security, the organisation's objectives must be examined in terms of the security requirements while considering, though, that there are usually limited resources available for implementing security safeguards. This is why it is especially important to identify the actual requirement on the availability, integrity and confidentiality of the information because a high level of security usually comes in conjunction with high implementation costs. It is also advisable to assign priorities to the requirements formulated if this is already possible at this point in time. The priorities are used as the basis for making resource planning decisions in later phases of the security process.

Notes on the detail of the description

It is not necessary in this early stage of the security process to examine all applications and IT systems in detail or perform a complicated risk analysis. It is more important to have an overview of which security requirements on the information technology result from the business processes or specialised procedures. For example, it should be possible to answer the following questions after determining the desired level of security:

- Which information is critical to the organisation in terms of its **confidentiality**, integrity, and availability?
- What critical tasks within the organisation cannot be performed at all, only performed inadequately, or only with considerable additional effort without IT support?
- What essential decisions made in the organisation rely on the confidentiality, integrity, and availability of information and information processing systems?
- What are the possible effects of deliberate or unintentional security incidents?
- Are the IT systems used to process information which requires special protection due to its confidentiality?
- Do key decisions depend on the correctness, up-to-dateness, and availability of the information processed by the IT?
- Which legal requirements (for example for data protection) result in special **safeguards**?

The descriptions of the desired level of security should be adapted according to the actual environment. Providing brief reasons is helpful in encouraging the resulting safeguards. For example, for a hospital this could mean: "a high level of information security is essential in the X-ray department because the lives of people depend on the correct operation of the IT systems."

Action Points for 3.2 Designing and Planning the Security Process
▪ Appoint contact persons for all business processes and specialised tasks ▪ Perform a rough assessment of the value of the information, business processes, and specialised tasks ▪ Determine the general requirements ▪ Estimate the importance of the business processes, specialised tasks, and information ▪ Specify the general information security objectives ▪ Obtain the agreement of management

3.3 Creation of a policy for information security

The information security policy describes in general terms how information security is to be established in the organisation, for which purposes and with which resources and structures. They contain the information security objectives desired by the organisation and the security strategy to be followed. The security policy therefore also describes the desired level of security in a government agency or company through the security objectives. It is therefore both an assertion and a statement that this level of security is to be obtained at all levels in the organisation.

The security policy is created by following the steps below:

3.3.1 Responsibility of management for the security policy

The policy for information security documents the strategic position taken by the organisation’s management to achieve the information security objectives in all levels of the organisation

Since the security policy represent a central strategy paper for information security in an organisation, it must be designed so that all organisational units can identify with its contents. Therefore, as many departments as possible should be involved in its preparation. Note, though, that each organisation must ultimately decide for themselves which departments and hierarchical levels will be involved in formulating the security policy.

When creating the security policy, it is recommended to use the expertise available in the following organisational units: the specialists responsible for important applications, IT operations, and security (information, IT, and infrastructural security); the Data Protection Officer; personnel department; staff council or supervisory board; auditing; finance department representatives; the legal department

3.3.2 Specifying the scope and contents of the security policy

The information security policy must state which areas it applies to. The scope may include the whole organisation or just parts of the organisation. It is important, though, that the scope fully include the business tasks and processes examined. Specifying the scope is not always a trivial task, especially for larger organisations. Specifying the scope according to areas of responsibility may be helpful.

The security policy should be formulated clearly and briefly because policy papers containing more than 20 pages have not been successful in actual practice. The policy paper should contain at least the following information:

- The value placed on information security and the importance of the main information and IT to perform the tasks

- The relationship between the information security objectives and the business objectives or tasks of the organisation
- The security objectives and the core elements of the security strategy for the IT used
- A guarantee that the security policy is implemented by the organisation's management together with key statements on monitoring success
- A description of the organisational structure established to implement the information security process

In addition, the following statements could be added, for example:

- For motivational reasons, some of the main threats to the business processes may be sketched, and the most important legal regulations and other important conditions (such as contractual agreements) may be stated.
- The key tasks and responsibilities in the security process should be pointed out (especially those of the IS management team, the IT Security Officer, IT users, and IT administrators). In addition, the organisational units or roles who will act as contact persons for security issues should also be stated.
- Programmes to promote information security through training and awareness-raising activities could also be announced.

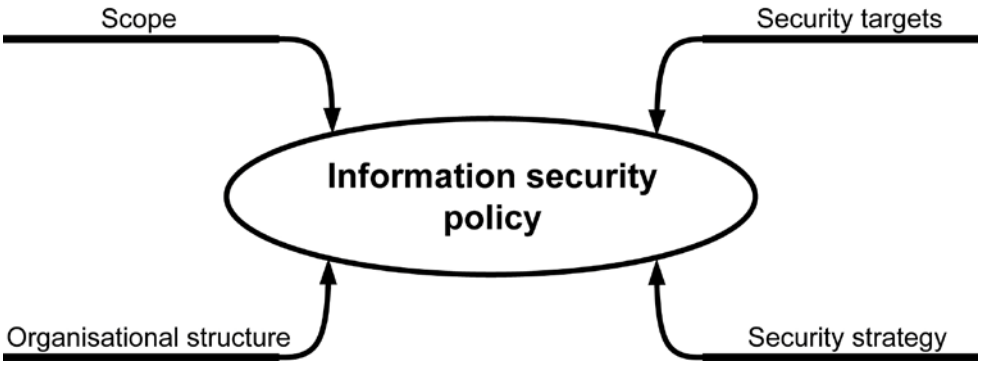


Figure 2: Contents of the security policy

3.3.3 Summoning a development team for the security policy

If an IS Management Team already exists in the organisation, then this team should be responsible for developing, reviewing, and revising the information security policy. The draft document is then submitted to the administration and management, respectively, for approval

If the information security management team is still being put together, then a development group should be established to draw up the information security policy. This group can assume the function of the IS Management Team as the security process proceeds. It is advisable for this development group to include representatives of the IT users, the IT operational staff, and one or more additional employees who have had sufficient training in information security. Ideally, a member of management who is able to assess the importance of information processing for the organisation should also be added to the team for a while.

3.3.4 Releasing the security policy

It is important that the administration or management underlines its objectives and expectations by publishing the security policy and emphasizes the value and importance of information security throughout the entire organisation. For this reason, all employees should know and understand the contents of the security policy. The security policy should be explained to new employees before they are granted access to the information processing systems.

Since the administration or management is ultimately responsibility for the information security policy, the policy should be specified in writing. The security policy must be formally approved by the administration or management. The contents of the security policy should not only be known within the organisation, but also be accessible as easily as possible, for example on the organisation's Intranet. If they contain confidential information, then this information should be placed in an Appendix that is clearly marked "confidential"

Finally, all members of staff should be made aware of the fact that committed, co-operative, and responsible action is expected of them not only with regard to the fulfilment of tasks in general, but also with regard to the fulfilment of the "information security" task.

3.3.5 Updating the security policy

The policy for information security should be checked and updated if necessary at regular intervals. For example, the organisation should consider if any business objectives or tasks, and therefore business processes or IT procedures, have changed; if the organisational structure has been altered; or if new IT systems have been introduced. Due to both the rapid developments in the field of IT and the security situation, it is recommended to revise the security policy at least every two years.

Action Points for 3.3 Creating the security policy
▪ Obtain a request from management to develop the security policy
▪ Specify the scope
▪ Summon a development group for the security policy
▪ Organise management approval of the security policy
▪ Release the security policy
▪ Check the security policy regularly and update if necessary

3.4 Organisation of the security process

The desired level of security can only be achieved if the information security process is implemented throughout the entire organisation. The global character of the security process means it is necessary to specify roles in the organisation and assign the corresponding tasks to these roles. These roles must then be assigned to qualified employees who will perform the required tasks. This is the only way to ensure that all important aspects will be taken into account and that all tasks will be performed efficiently and effectively.

The organisational structure required to promote and enforce the implementation of the information security process is referred to as the information security organisation, or IS organisation for short.

The number of people dealing with information security, the organisational structures they belong to, and resources required depend on the size, nature, and structure of the corresponding organisation. In any case, an IT Security Officer must be appointed as the key contact person for the co-ordination, administration, and communication of the information security process. In large organisations, there are usually additional people who perform a variety of sub-tasks relating to information security. To co-ordinate the activities of these people, an IS Management Team should be established that handles all generic information security issues and works on plans, policies, and guidelines.

In order to secure direct access to the organisation's administration or management, these roles should be organised as staff positions. At management level, the information security role should be clearly assigned to one manager to whom the IT Security Officer then reports.

Regardless of how to optimally structure the IS organisation, the following three basic rules must be followed.

Basic rules for defining roles in information security management

- The overall responsibility for the proper and secure completion of tasks (and therefore for information security) remains with the management.
- At least one person is to be appointed (usually as the IT Security Officer) to promote and co-ordinate the information security process.
- Every employee is equally responsible for their regular tasks and for maintaining information security at their workplace and in his or her environment.

3.4.1 Integrating information security into organisation-wide procedures and processes

Information security management is only one of many management tasks, but it has an influence on almost every area of an organisation. For this reason, information security management must be appropriately integrated into the existing organisational structures, and a contact person must be appointed. The tasks must be clearly separated from the responsibilities. In this context, it must be ensured that all necessary security aspects have been taken into account (for example the aspects of outsourcing or the use of electronic sales channels) not only for individual safeguards, but also when making all strategic decisions. In order to ensure this, it is important to involve the IS organisation at the proper time in all projects that could affect information security.

In larger organisations in particular, there is often already a global risk management system implemented. Since IT risks are among the most important operational risks, the methods of managing IT risks must be co-ordinated with the methods that have already been established.

3.4.2 Structure of the information security organisation

Depending on the size of the organisation, there are various ways to structure an organisation for information security management.

The following figures show three of these possibilities. The first figure shows the structure of the IS organisation in a large organisation. The second figure shows the structure in a medium-sized organisation in which the IS Management Team and IT Security Officer roles are combined. The third figure shows a structure for the IS organisation in a small organisation in which the IT Security Officer performs all tasks.

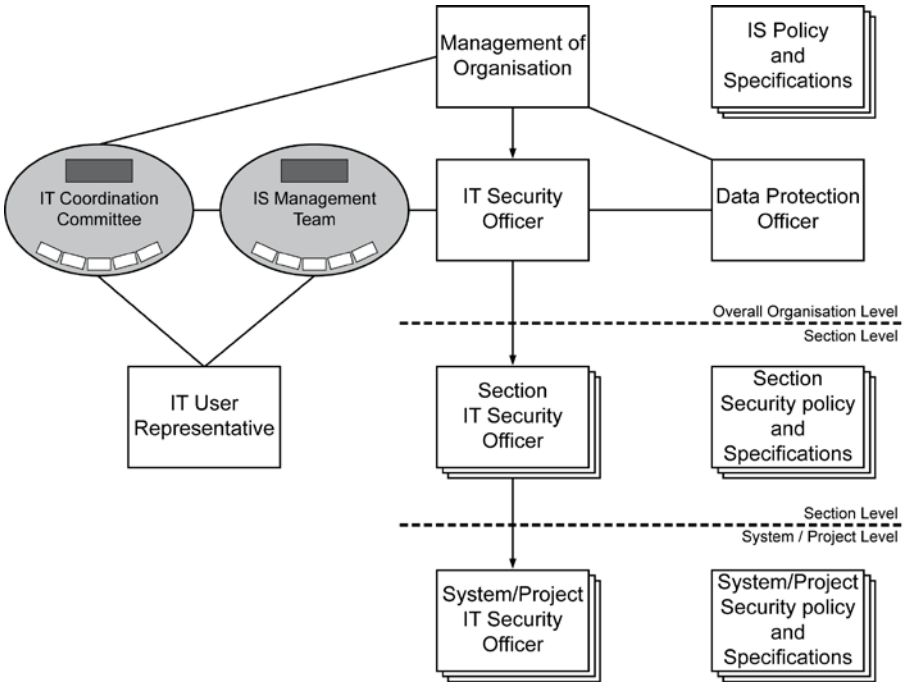


Figure 3.1: Structure of the IS organisation in a large organisation

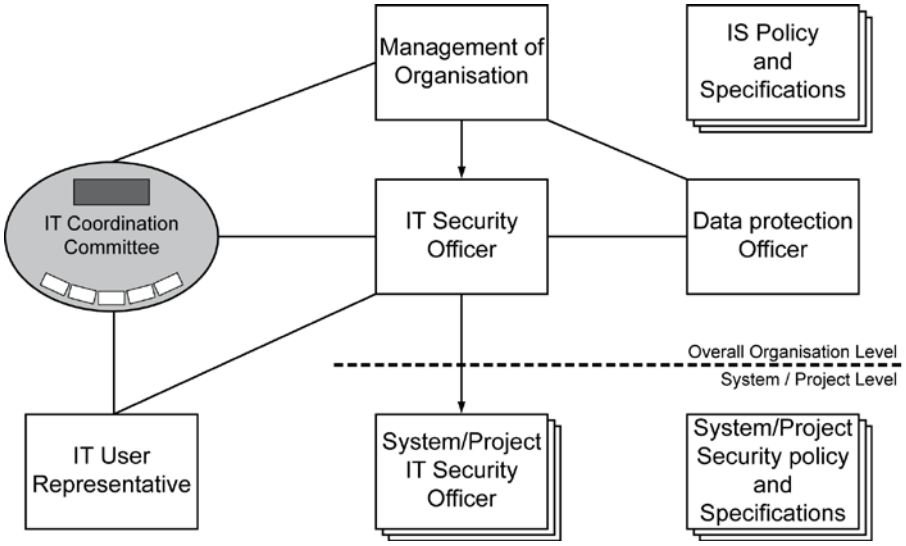


Figure 3.2: Structure of the IS organisation in a medium-sized organisation

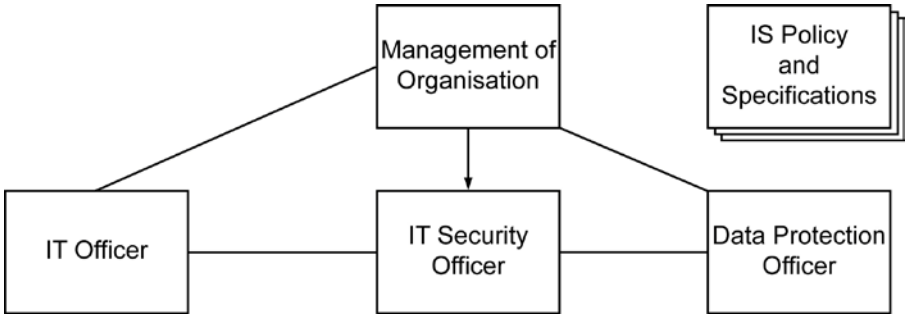


Figure 3.3: Structure of the IS organisation in a small organisation

At this point, it should be clearly emphasised that the main roles shown in these figures do not necessarily need to be assumed by different people. The personnel arrangements should depend on the size of the corresponding organisation, the available resources, and the desired level of security. The resources for supporting information security must be planned so that the level of security agreed to can actually be reached.

3.4.3 Tasks, responsibilities, and authorities in the IS organisation

The IT Security Officer and the IS Management Team must have clearly defined tasks, responsibilities, and authorities that are specified by management. In order to be able to perform their tasks, they should both be involved in all relevant procedures and in all decisions. The roles should be integrated into the organisational structure so that all those involved are able to communicate with each other. The IT Security Officer role and membership in the IS Management Team should be entrusted to qualified personnel. If necessary, some tasks can be delegated to the departmental IT Security Officers, IT Project Security Officers, or IT System Security Officers for additional support.

3.4.4 The IT Security Officer

Information security is frequently neglected, which means it is usually secondary to day-to-day business operations. If the responsibilities are not clearly separated, then there is a risk that information security becomes "someone else’s problem". The result is that the responsibility for information security is passed around from one person to the next until everyone believes someone else has the responsibility. To avoid this, a main contact person for all aspects of information security, i.e. an IT Security Officer, should be appointed to promote and co-ordinate the task of information security in the organisation. Whether or not there are additional people other than the IT Security

Officer who also have security roles and how information security is organised depends on the type and size of the organisation.

The actual name of the role fulfilling the responsibility for information security will differ depending on the type and nature of the organisation. Common titles include IT Security Officer or ITSO, Chief Security Officer (CSO), Chief Information Security Officer (CISO), or Information Security Manager. The "Security Officer" title, though, often designates the person responsible for occupational safety, operational safety, or factory safety.

In order to successfully plan, implement, and maintain a security process, the responsibilities must be clearly defined. Roles must be defined that will perform the various tasks required to achieve the information security objectives. In addition, qualified people must be appointed to fill out these roles, and these people must be provided sufficient resources.

Responsibilities and tasks

The IT Security Officer is responsible for handling all information security issues in the organisation. The main job of the IT Security Officer is to advise the administration or management in how to fulfil their roles in terms of information security and to help them perform these roles. The task of the IT Security Officer include, among others:

- Controlling the information security process and participating in all tasks relating to it
- Providing management with support when creating the policy for information security
- Co-ordinating the creation of the security concept, the contingency planning concept, and other sub-concepts and system security guidelines as well as issuing additional guidelines and rules for information security
- Initiating and monitoring the implementation of security safeguards,
- Informing management and the IS Management Team of the current status of information security
- Co-ordinating projects relating to security
- Investigating security incidents
- Initiating and co-ordinating awareness-raising and training safeguards for information security

The IT Security Officer is also involved in all large projects having a significant effect on the processing of information and in introducing new applications and IT systems in order to ensure that the security aspects are taken into account in the various phases of the project.

Requirements profile

To perform these tasks, the IT Security Officer should preferably have knowledge and experience in the fields of IT and information security. Since this task requires a variety of skills, the person appointed to this position should also have the following qualifications:

- The person should identify with the information security objectives and have an overview of the tasks and objectives of the organisation,
- The person must be able to co-operate and work in a team, but also be assertive (there are few tasks requiring such skills and ability in dealing with other people: management must be integrated again and again into a number of the main phases of the security process, decisions must be obtained, and the employees must be integrated into the security process, eventually with the help of the IT Security Officer of the corresponding department)
- The person should have project management experience, ideally in the fields of system analysis, as well as knowledge of methods for risk assessment

An IT Security Officer must also be willing to learn about new subjects and follow developments in IT. This role also requires additional and supplemental training so that the person has the expert knowledge required to perform the tasks.

Co-operation and communication

Working with the employees and external personnel requires a high degree of skill since these people must first be convinced of the necessity of the security safeguards, which some may perceive as a burden. An equally sensitive subject is the questioning employees after critical security incidents or about weaknesses critical to security. In order to guarantee success here, the employees must be convinced that honest answers will not cause any problems for them.

IT Security Officers require excellent communication skills not only when talking to employees. It is equally important that they are able to advocate their expert opinions when talking to the administration or management. They must therefore be self-confident and able to communicate so that they can occasionally raise objections to decisions incompatible with the objective of obtaining secure IT operations.

Independence

It is recommended to establish the IT Security Officer position organisationally as a staff position, meaning a position placed directly in the management level and which does not receive orders from any other position. For example, it is problematic when an "active" administrator assumes this role in addition to his normal tasks because there is a high probability of a conflict of interests. Having a single person assume both roles can lead to situations in which the person, as the IT Security Officer, would have to object to decisions that would make his or her work much easier or that are strongly favoured by their superiors. In any case, the IT Security Officer must have the right to speak directly to the administration or management at any time in order to inform them of any security incidents, security risks, and safeguards. This person must also be informed quickly and in full of any events in the organisation relevant to his or her job as IT Security Officer.

Combining the IT Security Officer and Data Protection Officer roles

A frequent question is whether or not the IT Security Officer can also assume the role of the Data Protection Officer (for more information on this position, see below). 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. In addition, both roles should have direct reporting routes to the management level. There should also be consideration as to whether the auditing department is informed of highly contested issues.
- The IT Security Officer must have adequate resources to assume both roles. If necessary, the role must be provided support by the corresponding agents.

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

3.4.5 The IS Management Team

The IS Management Team supports the IT Security Officer by co-ordinating the safeguards global to the entire organisation, collating information, and carrying out monitoring tasks. The actual form of the team depends on the size of the corresponding organisation, the desired level of security, and the available resources. In extreme cases, the IS Management Team consist of only one person, the IT Security Officer, who is responsible in this case for all the tasks in the security process.

The tasks performed by the IS Management Team include, in particular:

- Specifying information security objectives and strategies, and developing the policy for information security
- Checking the implementation of the information security policy
- Initiating, controlling, and monitoring the security process

- Helping to create the security concept
- Checking if the security safeguards planned in the security concept function as intended and if they are appropriate and effective
- Designing the training and awareness-raising programmes for information security
- Advising the IT Co-ordination Committee and management on questions relating to information security

Composition of the team

In order to be able to perform its tasks, the members of the IS Management Team should have knowledge of information security, technical knowledge of IT systems, and experience in organisation and administration. In addition, the IS Management Team should reflect the different operational areas of the organisation. The following roles should be represented in the IS Management Team at a minimum: a person responsible for IT, the IT Security Officer, and a representative of the users. Since personal data is often affected, the Data Protection Officer should also be a member of the IS Management Team. If a similar body already exists in the organisation, then its set of tasks could be extended accordingly. To underline the importance of information security, it is advisable to set up an IT Security Management Team and to provide it with sufficient resources.

3.4.6 Area IT Security Officer, Project Security Officer, and IT System Security Officer

In large organisations, it may be necessary to employ separate IT Security Officers in each of the various business units (referred to below as "Area IT Security Officers"). The Area IT Security Officer is responsible for all security issues relating to business processes, applications, and IT systems in his or her area (e.g. in a department or branch office). Depending on the size of the business unit, the task of the Area IT Security Officer can be assumed by someone who is already entrusted with similar tasks, e.g. the person is already the Departmental IT Officer (if such a position exists). In any case, it must be ensured when selecting the Area IT Security Officers that they are very familiar with the tasks, conditions, and work procedures in the relevant business unit.

The various business processes, applications, and IT systems in an organisation often have different security requirements which, under some circumstances, may already be recorded in specific security policies and which may require different security safeguards. The situation is similar for the Project Security Officer except for the fact that this person’s tasks are project-specific and instead of IT system-specific.

The tasks to be assigned to the Project, System, and Area Security Officers include:

- Implementing the rules and regulations specified by the IT Security Officer
- Implementing the security safeguards according to the IT system security policy or some other, more specific security policies,
- Gathering IT system-specific information and forwarding it to the IT Security Officer
- Acting as on-site contact person for the employees
- Being involved in the selection of the security safeguards used to implement the specific security policy,
- Obtaining information on the need for training and awareness-raising for the employees
- Monitoring and evaluating log files at regular intervals
- Notifying the IT Security Officer of any security-related problems

Requirements profile

The following qualifications are necessary for these roles:

- Detailed knowledge of IT since this makes it easier to talk to the employees on-site and is useful when searching for security safeguards for special IT systems
- Knowledge of project management, which is helpful when organising user surveys and drawing up plans for the implementation and monitoring of security safeguards

3.4.7 IT Co-ordination Committee

The IT Co-ordination Committee is generally not a permanent committee in an organisation but is summoned as required (e.g. for planning larger IT projects). Its task is to co-ordinate the interaction between the IS Management Team, the IT user representative, the IT Security Officer, and administration or management.

3.4.8 The Data Protection Officer

Data protection is often treated as secondary since it allegedly hinders the effective processing of information even though data protection is prescribed in Germany and many other countries through legal regulations and violating the resulting informational self-determination rights can lead to serious fines and prison sentences.

The Data Protection Officer job is often assigned to persons who already fulfil a different role and whose new function can result in conflicts of interest, for example when the new function means they themselves will be controlling their original function (as is the case with the head of the IT department).

To avoid this situation, a competent and qualified contact person should be assigned to respond to questions relating to data protection, who accompanies all aspects relating to data protection in the org, and who ensures the protection is properly implemented and adequately checked. In this function, this person works closely with the IT Security Officer, is a member of the IS Management Team, is able to make decisions independently, and reports directly to the administration or management.

When appropriately realised, data protection will more likely promote the work procedures than hinder them. If, for example, a government agency or company collects too much personal data, deletes personal data too late, or transfers it without authorisation to third parties, then they are not only violating the data protection laws, but also increasing the amount of administration required and generating higher costs. In particular, data protection is an important part of good conduct with citizens and customers alike because it makes the procedures more transparent.

Every organisation should appoint a Data Protection Officer. For many areas, the laws even require the installation of a Data Protection Officer. Even organisations that have not appointed a Data Protection Officer must ensure that the legal data protection requirements are fulfilled. This can also be ensured by the IS Management Team or the internal auditing department.

Requirements profile

Only persons who possess the required knowledge to perform these tasks and are dependable can be appointed as the Data Protection Officer. Technical, organisational, and legal knowledge are required to perform the corresponding tasks. The Data Protection Officer must know and be able to securely apply the corresponding legal regulations, area-specific data protection laws and regulations, and the relevant special rules and regulations of the organisation. One particularly important legal standard in Germany is the German Federal Data Protection Act. The Data Protection Officer should also be familiar with the organisation and possess in-depth knowledge of information technology. If any qualifications are missing in some areas, then this person must be given the opportunity to obtain further training accordingly. The Data Protection Officer should be familiar with the government agency or company from his or her own experience so that this person can perform the required control and consulting tasks properly.

The Data Protection Officer does not have to be this person’s only function. Depending on the type and amount of personal data processed and the data protection problems associated with this

processing, it may be appropriate to assign additional tasks to this person. This applies especially to small organisations. Special care must be taken to ensure that no conflicts of interest or dependencies are created that could endanger this person's ability to perform the required tasks. It is also possible to merge the Data Protection Officer and IT Security Officer functions.

Inclusion duty

The Data Protection Officer must have the right to speak directly and at any time to administration or management, and must also be informed quickly and in full of any events in the organisation relevant to his or her activities as the Data Protection Officer. This person must be allowed to participate in operations relevant to data protection and must be informed of any plans affecting the handling of personal data. If necessary, this person must be provided with support by other employees having more extensive legal or technical knowledge.

Responsibilities and tasks

The Data Protection Officer should contribute to the efforts to ensure that the organisation completely fulfils the data protection requirements. This person must monitor all areas to ensure that the data protection regulations are followed. This is achieved primarily through checks and by consulting with employees. The primary task is providing advice. For the employees, the Data Protection Officer is a contact person who they can turn to at all times for all questions relating to data protection. If weaknesses or errors are found, then he should look for a constructive solution together with the employees.

The Data Protection Officer helps administration or management to fulfil their responsibility to protect people's privacy and prevent incidents which could reflect poorly on the reputation of the organisation. He should also be in contact with the staff council and supervisory board. Good interaction is not only desired due to the confidential nature of the personal data processed.

The actual tasks performed by the Data Protection Officer depend in each case on the requirements to be met, but also on the size, organisational structure, and division of responsibilities in the corresponding government agency or company.

Action Points for 3.4 Creating the IS organisation
▪ Specify roles for designing the information security process
▪ Assign tasks and areas of responsibilities to the roles
▪ Specify the human resources required for the roles
▪ Document the IS organisation
▪ Integrate information security management into the organisation-wide processes and procedures

3.5 Providing the resources for information security

Threats may result in damage and therefore incur costs, but preventing risks also requires resources – effective risk management helps control these costs. An appropriate level of information security can only be achieved and maintained with the appropriate expenditures. For this reason, it must be ensured when specifying the desired level of security and formulating specific security requirements for the organisation that the desired level of security is also economically feasible.

3.5.1 Cost-efficient security strategy

Cost-effectiveness must be considered right from the start when designing the security strategy. If it becomes clear that the necessary security safeguards cannot be implemented with the resources available, then the strategy has to be changed. If the security requirements and financial capabilities

are incompatible, then the business processes and the way the IT is operated must be examined in general.

Experience has shown that the relationship between the expense required to increase the security level and the actual gain in security attained through this expense leads to diminishing returns as the desired security level increases. It is not possible to achieve perfect information security. The following diagram should help clarify the how the expense relates to the desired level of security. The expense obtained from the diagram can be used as a basis for determining the personnel, time, and financial resources required to achieve the desired level of security.

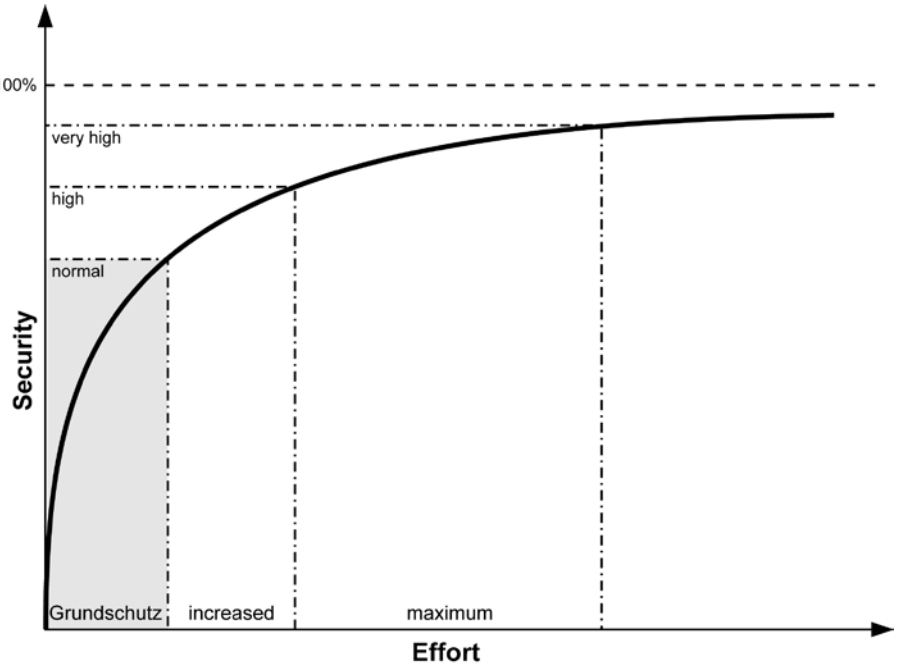


Figure 4: Cost/benefit relation for information security

It is absolutely essential that the cost/benefit aspects of each activity be examined closely when selecting the individual steps in the security process. Frequently, simple organisational rules that can be implemented without great additional cost or additional technical equipment make a substantial contribution to improving the security level. It only makes sense to invest in complex technical security infrastructures after these elementary security safeguards have been implemented.

Information security requires financial, personnel, and time resources, which must be provided by management in accordance with the requirements formulated. It is often the case that only technical solutions are considered for IT security. This is another reason why it is better to use the term "information security". Above all, it is important to point out that investing in human resources and organisational rules is often more effective than investing in security technology. Technology alone does not solve any problems since technical safeguards always need to be integrated into a suitable organisational framework.

3.5.2 Resources for the IS organisation

Information security surveys demonstrate that appointing an IT Security Officer is frequently the most effective security safeguard. After appointing an IT Security Officer, the number of security incidents in most organisations drops significantly. Above all, the IT Security Officer must be given enough time to perform his tasks. In small organisations, it is possible for one employee to assume the role of IT Security Officer parallel to his other roles.

Only a few organisations, either very large ones or ones with high information security requirements, will be able to create full-time staff positions in the IS Management Team. Normally, these tasks are be performed by the existing employees in addition to the employees' original duties. A possible

exception to this, however, is when the security process is set up for the first time. If possible, the members of the IS Management Team should be freed from their other duties for the most part during this phase. The decision as to whether staff should be released and to what extent will depend on how the tasks are divided between the IT Security Management Team and the IT Security Officer. The final decision for this rests with administration or management. In any case, the IS Management Team should meet regularly to ensure continual management of the security process.

Setting up an IS Management Team has the advantage that various organisational units can be integrated into the security process and skills can be bundled. This permits faster implementation of information security in all organisational units, and there is less friction as a result. The following organisational units may be involved in and co-ordinate the security activities, for example: Information security, auditing, IT administration, IT management, data protection, staff council/supervisory board, specialised departments, building services, legal department, finance department.

Access to external resources

In practice, the internal security experts often do not have enough time to analyse all the factors and prevailing conditions relevant to security (e.g. statutory requirements or technical questions). Sometimes they also lack the relevant fundamentals. In such cases, it is appropriate to refer to experts. This fact must be documented by the internal security experts so that the management level makes the necessary resources available.

Outsourcing some parts of IT operations or certain services, e.g. firewall operation, may increase information security when this permits access to specialists who are not available internally. Module 1.11 Outsourcing in the IT-Grundschutz Catalogues provides recommendations for what to consider from a security perspective.

3.5.3 Resources for monitoring information security

In addition, sufficient resources must be provided so that the effectivity and suitability of security safeguards can be monitored systematically. If possible, it should also be checked if the resources used are justified in terms of the level of security obtained. If, for example, it turns out that securing certain IT systems will result in unproportionally high costs, then alternative safeguards must be considered. It may be appropriate, for example, to ensure certain IT systems cannot connect to insecure networks if the cost of securing them up is too high.

3.5.4 Resources for IT operations

The basic requirement for secure IT operations is that the IT functions smoothly, i.e. that it is planned and organised properly. Consequently, adequate resources must be available for operating the IT systems. Typical problems encountered in IT operations (scarce resources, overburdened administrators, or an unstructured and poorly maintained IT landscape) generally need to be overcome so that the actual security safeguards can be implemented effectively and efficiently.

Action Points for 3.5 Providing the resources for information security
▪ Consider the factors of appropriateness and cost-effectiveness throughout the security process
▪ Ensure there is a balance between organisational and technical information security
▪ Request appropriate resources for IT operations, for information security management, and for monitoring the information security
▪ If necessary, utilise external resources

3.6 Integration of all employees in the security process

Information security affects all employees without any exceptions. Each individual, through responsible and security-conscious actions, can help avoid damage and thus contribute to the success of the organisation. For this reason, increasing the level of awareness for information security and special training for the employees is a basic requirement for information security. The working climate, common values, and the motivation of the employees also have a decisive effect on information security.

For all employees, whether internal and external, information security issues must be considered from the time the person is selected for a position to their departure from the organisation.

3.6.1 Training and raising awareness

All employees must be trained in and have an increased awareness of the importance of security safeguards and their application. That is why training concepts must be created for a range of target groups (e.g. administrators, managers, users, security guards). Information security training must be integrated into the existing training concepts.

All employees who are new to the company or have been assigned new tasks should receive thorough training and instruction. All relevant security issues should be integrated into the design and selection of the relevant training safeguards. Experienced IT users should also refresh and add to their knowledge regularly.

The level of awareness of the employees for information security issues must be increased regularly in order to sharpen their awareness for risks when handling information on a daily basis. In order to effectively achieve an increased level of awareness for information security, it may be appropriate, for example, to set up a security forum in the intranet in which tips on security safeguards and current security incidents are published, to offer employees workshops or presentations on information security, or to provide technical magazines.

3.6.2 Communication, integration, and reporting routes

In order for employees to remain aware of security issues even after training and awareness raising safeguards, it is important to appoint a contact person for security questions and to inform every one of these responsibilities. This is the only way to actively support the employees and to implement security policies and concepts in practice over the long term. This includes defining reporting and escalation routes for security incidents. Every employee must know how to act when he or she suspects a security incident has occurred and who to contact in this case. In addition, it must be possible to obtain this information quickly and under all circumstances, even when no IT is available, for example.

Employees must understand the reasons for the security safeguards. This is particularly important if they have a negative affect on comfort or function. In come cases, security safeguards may require by law the approval and participation of the staff council or supervisory board.

There are several advantages of involving the employees in an early stage when planning security safeguards or designing organisational rules:

- The organisation's existing knowledge and ideas can be better exploited.
- This increases the practicality and efficiency of security safeguards or organisational rules
- There willingness to actually follow the rules and security safeguards in everyday operations increases.
- It has a positive effect on the working climate because employees feel involved in the decisions made by management

3.6.3 When employees leave or switch jobs

When employees leave, switch jobs, or lose areas of responsibility, the process must be accompanied and documented by appropriate security safeguards. In general, there are several locations in an organisation that need to be informed when an employee leaves the organisation or switches to a different job in the organisation, and corresponding action must be taken (for example, keys and passes must be returned, the access rights to applications and information need to be changed, the gatekeepers and other personnel need to be informed, etc. The identity and authorisation management must be clearly defined processes, for example in form of an instruction sheet or checklist, so that no security risks arise. If the employee had a function in the security process, then the corresponding documents, such as the contingency plan, must be updated accordingly.

Furthermore, it is advisable to inform the employees in advance (for example in the context of a service agreement) of their duties when switching jobs or when terminating their employment. This includes, among other things, informing them of their obligation to maintain secrecy.

Action Points for 3.6 Integration of all employees in the security process

- Involve the employees and staff council or supervisory board in the planning and design of security safeguards and rules at an early stage
- Train all employees in the relevant aspects of information security and raise their awareness regularly
- Explain the purpose of the security safeguards to all employees
- Specify a contact person for security questions and inform the employees of what this person is responsible for
- Specify and announce the reporting and escalation routes for security incidents
- Ensure that the required security safeguards are followed when an employee leaves or switches jobs.

4 Producing an IT Security Concept in accordance with IT-Grundschutz

One of the objectives of IT-Grundschutz is to offer a pragmatic and effective approach to achieving a normal security level that can also form the basis for a higher level of security. After initiating an information security process and defining the security policy and information security organisation, the organisation's security concept is created. The IT-Grundschutz Catalogues contains recommendations for this purpose in standard organisational, personnel, infrastructure, and technical security safeguards for typical components of business processes, applications, and IT systems. They are organised in modules so that they can build on each other.

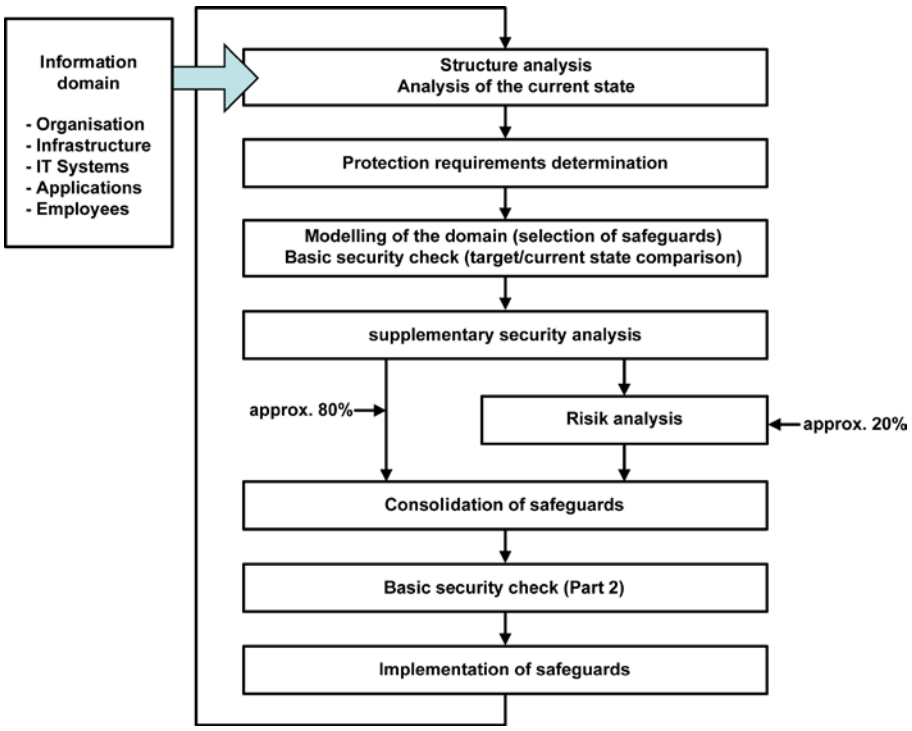


Figure 5: Creation of the security concept in information security management

The IT-Grundschutz Methodology

In the traditional risk analysis approach, the threats are identified first and assigned a probability of occurrence so that suitable security safeguards can be selected and the residual risks can be evaluated. In IT-Grundschutz, this step has already been taken for every module, and the appropriate security safeguards are selected for typical application scenarios. When applying IT-Grundschutz, this task is reduced to an analysis comparing the security safeguards recommended in the IT-Grundschutz Catalogues to those already implemented. Safeguards found to be missing or inadequately implemented reveal security deficits that can be eliminated by implementing the recommended safeguards. Only where the protection requirements are significantly higher is it necessary to perform a supplementary security analysis which takes the costs and effectiveness of implementing additional safeguards into account. In general, it is sufficient to supplement the recommended safeguards in the IT-Grundschutz Catalogues with the corresponding individual, higher-quality safeguards. A procedure simpler than the traditional risk analysis methods used for this purpose is described in BSI Standard 100-3 "Risk Analysis on the Basis of IT-Grundschutz" [BSI3].

The IT-Grundschutz Methodology is roughly divided into the following areas:

Defining the scope

Implementing IT-Grundschutz in one single large step is frequently too ambitious. Many small steps and a long-term, continuous process of improvement without high initial investment costs are often more successful. It may therefore be better to implement the necessary level of security only in selected areas at first. The security of the whole organisation can then be continuously improved on starting from this base level.

Therefore, the areas for which the security concept will be created and to which it will apply must be specified first. These areas may be certain organisational units in an organisation, for example, but could also include areas that handle defined business processes or specialised tasks, including the necessary infrastructure.

In IT-Grundschutz, the area to which the security concept applies is also referred to as the "information domain".

Structure analysis

To produce a security concept, and in particular when applying the IT-Grundschutz Catalogues, it is necessary to analyse and document the interaction between the business processes, the applications, and the existing information technology. Given that IT systems today are usually highly networked, the use of a network topology plan is recommended as the starting point for further analysis. The following aspects must be considered:

- The applications operated in the information domain and the business process supported by these applications
- The organisational and personnel framework for the information domain
- The IT systems used in the information domain, both networked and non-networked
- The communication links between the IT systems and the outside world
- The existing infrastructure

Each step in the structure analysis is described in detail in Section 4.2 of this document in the form of instructions.

Determining the protection requirements

The purpose of the protection requirements determination is to assess the level of protection that is adequate and appropriate for the business processes, the information processed, and the information technology used. For each application and the information processed with it, the potential damage which could occur as a result of the loss of confidentiality, integrity, or availability must be assessed. It is important to realistically assess any possible consequential damage. Classification into the three protection requirements categories "normal", "high", and "very high" has proven successful in the past.

The individual steps in defining the protection requirements are described in detail in Section 4.3 of this document.

Selection and adaptation of safeguards

Detailed documents on the structure and the information domain and its required protection level are a prerequisite for applying the IT-Grundschutz Catalogues to the information domain. This information should be obtained before performing the steps described. To identify suitable security safeguards for the information domain examined, the modules in the IT-Grundschutz Catalogues only need to be associated with the corresponding target objects and subsections.

This part of the modelling process is described in detail in section 4.4.

Basic security check

The basic security check is an organisational tool which provides a quick overview of the existing security level. Interviews are used to establish the current status of an existing information domain

(modelled according to IT-Grundschutz) in terms of the extent to which the IT-Grundschutz security safeguards have been implemented. The outcome of this check is a catalogue in which the implementation status of each of the relevant safeguards is classified as "Yes", "Partially" or "No". By identifying safeguards which have not yet been implemented or have only been partially implemented, it is possible to point out where there is room for improvement in the business processes and information technology being examined.

Section 4.5 describes an action plan for performing a basic security check. It takes both the organisational aspects and the technical requirements during project implementation into account.

Additional security safeguards

The standard IT-Grundschutz security safeguards provide appropriate, adequate protection for normal operation. However, if the protection requirements are high or very high, it may be appropriate to check if even higher quality security safeguards are needed. This also applies when there are special application conditions present or when components which cannot be modelled with the existing modules in the IT-Grundschutz Catalogues. It must first be decided in the context of a *supplementary security analysis* if a risk analysis needs to be performed for each of the affected areas.

One method for risk analysis is the procedure described in BSI Standard 100-3 "Risk analysis based on IT-Grundschutz". An overview of this method is provided in section 4.6. The successful execution of a risk analysis depends decisively on the expertise of the project team. It is therefore often helpful to employ external specialists.

4.1 Defining the scope

Before creating a security concept, the areas of the organisation to which it will apply must be specified first, i.e. the scope of the security concept must be defined. The scope of the security concept can be identical to the scope of the policy for information security, but it may also make sense to develop security concepts for smaller areas. This could be the case, for example, when the initial estimate of the total expense of implementation is too high and certain business processes must be handled according to their priorities according to the security policy.

Not only technical aspects should be taken into account when defining the scope, but also organisational aspects so that the areas of responsibility and authorisations can be clearly defined. In any case, it should be clear which information, specialised tasks, or business processes will be examined explicitly in the security concept.

When defining the scope of the security concept, the following factors must be taken into account:

- The scope should contain all areas, aspects, and components used to support the specialised tasks, business processes, or organisational units and which are administered internally by the organisation.
- If this is not possible because parts of the specialised tasks or business processes depend organisationally on external partners, for example in the context of outsourcing, then the interfaces must be clearly defined so that they can be taken into account in the security concept as well.

Information domain

The scope of the security concept to be produced is referred to in the following as the "information domain" (or "IT system"). The term IT system, though, describes the scope from a technical perspective. An IT system not only has IT components assigned to it, but also information, organisational rules, operational areas and authorities, as well as physical infrastructure components. This is why the term “information domain” is more appropriate.

An information domain consists in this case of all the infrastructural, organisational, personnel, and technical components required to perform the tasks in a certain area of application of the information

processing. An information domain can refer to all aspects of information processing in an organisation or to individual areas organised according to organisational structures (e.g. departmental networks) or shared common business processes and shared applications (e.g. personnel information domains).

The components of the information domain under examination are documented and its structure is analysed to create the security concept. A systematic approach to the structure analysis is described in the next section.

Action Points for 4.1 Defining the scope of the security concept
▪ Specify which critical business processes, specialised tasks, or parts of an organisation will be included in the scope
▪ Clearly define the limits of the scope
▪ Describe interfaces to external partners

4.2 Structure analysis

The structure analysis is used to perform a preliminary survey of the information required for the additional procedures when creating a security concept according to IT-Grundschutz. In this case, this means documenting the components (information, applications, IT systems, rooms, communication networks) required to perform the business processes or specialised tasks specified to be in the scope.

To do this, the business-critical information and applications are determined, and the affected IT systems, rooms, and networks are recorded. In the classic approach, the applications are determined first, and then the objects affected by the applications are determined. One disadvantage of this approach is that it is often difficult to grasp the abstract applications without thinking about the actual technical components. For this reason, it may be more appropriate to change the order in this case and analyse the IT systems first since it is often easier to determine the applications based on the IT systems examined.
Note that the objects and data recorded in the context of a structure analysis are usually not only required for the security process, but also for operational aspects and administration purposes. It should therefore be examined if there are already databases or overviews available which could be used as sources of data for the structure analysis. In many organisations, databases are operated for inventory purposes, configuration management, or for designing business processes. This could lead to synergy effects.

The structure analysis is divided into the following sub-tasks:

- Documenting which business processes, applications, and information should be included in the scope
- Preparing a network plan
- Documenting the IT systems and similar objects
- Documenting the rooms

Note when performing all sub-tasks that it is often impractical to document every object individually. Instead, similar objects should be grouped together.

4.2.1 Reducing complexity by forming groups

The structure analysis provides important data for the entire security process. The information domain usually consists of a number of individual objects that all need to be taken into account when designing the concept. Even when all logical and technical objects have been documented, there is still a risk that the results of the structure analysis are unmanageable due to the large amount of data and its complexity. Similar objects should therefore be grouped accordingly.

For technical components, the formation of suitable groups also has the advantage of substantially simplifying the administration when there are just a few basic configurations. By obtaining the highest possible level of standardisation in an IT environment, you also reduce the number of potential security gaps, and the security safeguards for this area can be implemented without having to account for a wide variety of vulnerabilities. This not only benefits information security, but reduces costs as well.

Objects can then be assigned to one and the same group if all objects

- are of the same type,
- are configured in the same manner,
- are integrated into the network in the same manner (on the same switch in the case of IT systems, for example)
- are subject to the same basic administrative and infrastructural requirements
- operate similar applications, and
- have the same protection requirements.

Based on the prerequisites stated for forming groups, it can be assumed in terms of information security that the security status of a sample taken from a group represents the information security status of the entire group.

The most important example of a group of objects is surely the group of clients. Organisations generally have a large number of clients, but these clients can still be classified according to the scheme provided above into a reasonably small number of groups. The same applies to the rooms and other objects. In large information domains where, for reasons of redundancy or throughput, many servers perform the same task, it is perfectly reasonable to place these servers in a group.

The sub-tasks for the structure analysis are described in the following and explained using an appropriate example. A detailed version of the example can be found in the resources for IT-Grundschutz on the BSI web site. Objects should be collected in groups in all sub-tasks whenever this is appropriate and permissible.

Action Points for 4.2.1 Reducing complexity by forming groups
▪ Place all similar objects in a group when performing all sub-tasks of the structure analysis
▪ Note the type and number of each of the objects place in the group

4.2.2 Documenting the applications and related information

In this phase, the applications and information associated with every business process and every specialised tasks contained in the information domain must be identified. Applications are procedures that support the business processes and specialised tasks in government agencies and companies.

The degree of detail selected by the organisation for each of the applications examined is individual. The goal in this case it to obtain the highest possible transparency and efficiency when performing the structure analysis and determining the protection requirements. The modules examined in the IT-Grundschutz Catalogues in the applications layer could provide useful information for this step.

To further reduce the amount of work required, the structure analysis of the information domain can be limited to only those applications and information required for the business process or specialised tasks being examined. Care should be taken in this case so that, at a minimum, the applications and information required for the business processes or specialised tasks examined which need a minimum level of

- secrecy (confidentiality), or
- correctness (integrity), or

- availability

are taken into account.

In order to ensure this, the users and/or those responsible for the application and those responsible for the business processes should be asked for their assessment when documenting the applications used.

Due to the increasing complexity of applications, it is often unclear to the person responsible which dependencies exists between a business process or a specialised tasks and a specific application. Therefore, it must be determined which applications are necessary to perform every single specialised task and which data will be needed to perform this task. These dependencies could be determined in a meeting of the specialised departments, the persons responsible for each application, and the IT department.

If, in contrast to the order suggested here, the IT systems are documented first, then it is often helpful to determine the applications based primarily on the IT systems. Due to their widespread impact, information on the servers should be collected first. In order to achieve as balanced a picture as possible, this survey can then be completed by examining the clients and individual workstation systems. Finally, it must be determined which network switching elements support which applications.

The applications should be numbered so they can be associated with the corresponding information later. Since many IT Security Officers are also responsible for protecting personal data as the Data Protection Officer, it is useful to note at this time whether or not the applications described store and/or processes personal data. The protection requirement of an application generally results from the protection requirements of the data it processes. For this reason, the type of information should also be documented in a table.

It is also recommended to note which business processes the applications support. The person responsible for the application and its users should also be documented in order to more easily identify a contact person for security questions or to quickly reach the affected user groups.

When documenting the applications, it is recommended to examine the data media and documents as well and treat them like applications. When the data media and documents are not permanently linked to an application or an IT system, then the data media and documents must be integrated separately into the structure analysis. It does not make sense, of course, to document each data medium individually. Only those data media and documents with a minimum protection requirement should be examined, and groups should be formed whenever possible. Examples of data media and documents that should be documented separately during the structure analysis include:

- Archive and backup data media
- Data media used to exchange data with external communication partners
- USB sticks when used as portable devices
- Emergency manuals, which are available in printed form
- Microfilm
- Important contracts with partners and customers

Documenting the dependencies between applications

As an option, the dependencies between the applications can be illustrated to provide a better overview. For example, orders cannot be processed completely when there is no information on the warehouse stocks available.

It is recommended to document the results in a table or to use appropriate software products for this purpose.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 1

In the following, we present an example of how to document the applications determined in a fictitious government agency – the BOV. It should be noted that the structure of the BOV is by no means optimal in terms of information security. The example is simply used to illustrate how to proceed when applying IT-Grundschutz. Only an overview is provided here; the complete example is found in the resources for IT-Grundschutz.

The BOV is a fictitious government agency with 150 employees, and 130 of these employees have their own terminals. Geographically, the employees are divided between a main office in Bonn and an external location in Berlin where they handle such sub-tasks as principles, standards, and co-ordination. Of the 130 employees with IT-supported workstations, 90 work in Bonn and 40 in Berlin.

All the workstations are networked to enable the employees to perform their duties. The Berlin branch office is connected via a dedicated connection. Any employee can call up the basic guidelines, regulations, forms, and text modules they need at any time. All relevant results of their work are placed in a central database. Draft documents are prepared, distributed, and signed exclusively in electronic form. To implement and support all the necessary functionality, an IT department was set up in Bonn.

The business processes of the BOV are maintained electronically and are organised according to the following two-part scheme. The number of the main process is appended to the GP code, and the number of the subprocess follows after a hyphen, e.g. GP0-2.

The following contains an excerpt of which applications where determined to exist and the information associated with these applications for the fictitious BOV agency:

No.	Application	**Type of Information ***	Responsible	Users	Business Processes
A1	Processing of personnel data	P	Z1	Z1	GP0-1, GP0-2
A2	Benefits processing	P	Z2	all	GP0-2
A3	Travel expense accounting	P/A/S	Z2	all	GP0-1, GP0-3
A4	User authentication	P/T	IT1	all	GP0, GP5, GP6
A5	System management	T	IT3	IT3	all
A6	Office communication	P/A/S/T	IT3	all	all
A7	Central document administration	P/A/S/T	Z1	all	GP0, GP5
A8	USB sticks for use when exchanging data media	P/A/S	IT3	IT3	GP0-1, GP0-3

* Key:

- P = personal data
- A = administrative information of the BOV, for example the organisational structures and chains
  of command
- S = specialised information in the BOV, for example correspondence with customers
- T = Technical/system-related information, for example the configuration data of IT systems

The type of information is documented briefly here for each application so that the protection requirement for this application can be determined quickly based on the protection requirements of the information it processes. The categories used in the table above for the type of information are only examples and are not recommendations for categorising information.

Action Points for 4.2.2 Documenting the applications and related information
▪ Find out which applications are required for the business process being examined after consulting with the specialised department, the person responsible for the application, and the IT department providing support ▪ Create an overview of the applications and assign a unique number or code to each application ▪ For each application, note the relevant business processes, information processed, person responsible, and, if necessary, users ▪ For each application, note the extent to which it processes personal data

4.2.3 Preparing a network plan

A network plan (for example in the form of a network topology plan) can be a useful starting point for the further technical analyses. A network plan is a graphical representation of the components used in the IT and communications technology under consideration and of the manner in which they are networked together. Network plans and similar graphical overviews are usually available in most organisations since they are needed for operations. The plan should present a minimum of the following objects in terms of information security:

- IT systems, i.e. client and server computers, active network components (such as switches, routers, and WLAN access points), network printers, etc.
- Network connections between these systems, i.e. LAN connections (such as Ethernet or token ring), WLANs, backbone technologies (such as FDDI, ATM), etc.
- Connections between the area being examined and the outside world, i.e. dial-in access over ISDN or modem, Internet connections using analogue technologies or routers, radio links or leased lines to remote buildings or property, etc.

For each of the objects represented, there should also be a minimum set of information available which can be obtained from an assigned catalogue. As a minimum, the following information should be noted for each IT system:

- A unique name (for example the full host name or an identification number)
- The type and function (e.g. database server for application X)
- The underlying platform (i.e. hardware platform and operating system)
- The location (e.g. building and room number)
- The administrator responsible
- The available communication interfaces (e.g. Internet connection, Bluetooth, WLAN adapter)
- The type of network connection and the network address

Certain information is needed not only for the IT systems themselves but also for the network connections between the systems and for connections to the outside world, including:

- The type of cabling or communication link (e.g. fibre optic cables or WLAN based on IEEE 802.11)
- The maximum data transmission rate (e.g. 100 Mbps)

- The network protocols used on the lower layers (e.g. Ethernet, TCP/IP)
- For external connections, details of the external network (e.g. Internet, name of provider)

Virtual IT systems and virtual network connections, for example Virtual LANs (VLANs) or Virtual Private Networks (VPNs) should also be represented in a network plan when the logical (virtual) structures implemented differ significantly from the actual physical structures. It may be appropriate for reasons of clarity to diagram the logical (virtual) structures in a separate network plan.

It is recommended to indicate areas with different protection requirements.

The network plan should be created and maintained in electronic form whenever possible. If the amount of information technology in the organisation has extended a certain limit, it may be appropriate to use a suitable utility program to document and maintain the network plan since this document can be very complex and is subject to constant change.

Updating the network plan

Since the IT structure is generally adapted to the specific requirements of the organisation and maintenance of the network plan binds the corresponding resources, the network plan for the organisation may not always be up-to-date. In practice, the plan is usually only updated after major changes to the IT structure of specific areas have been made.

With regard to using the network plan for the IT structure analysis, the next step consists of comparing the existing network plan (or partial plans, if the overall plan has been divided into smaller sections to make it easier to read) to the actual IT structure present and updating it to reflect the current state, if necessary. When updating the plan, those responsible for IT and any administrators of individual applications and networks should be consulted. If any programs are used for centralised network and system management, it should always be checked if these programs provide any support for the creation of network plans. However, it should be noted that functions for the automatic or semi-automatic detection of components will temporarily generate additional network traffic. Steps must be taken to ensure that this network traffic does not impair IT operations. In addition, the results of automatic or semi-automatic detections must always be checked to ensure that all relevant components were actually detected.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 2

The following shows an example of a network plan for a fictitious government agency, the BOV.

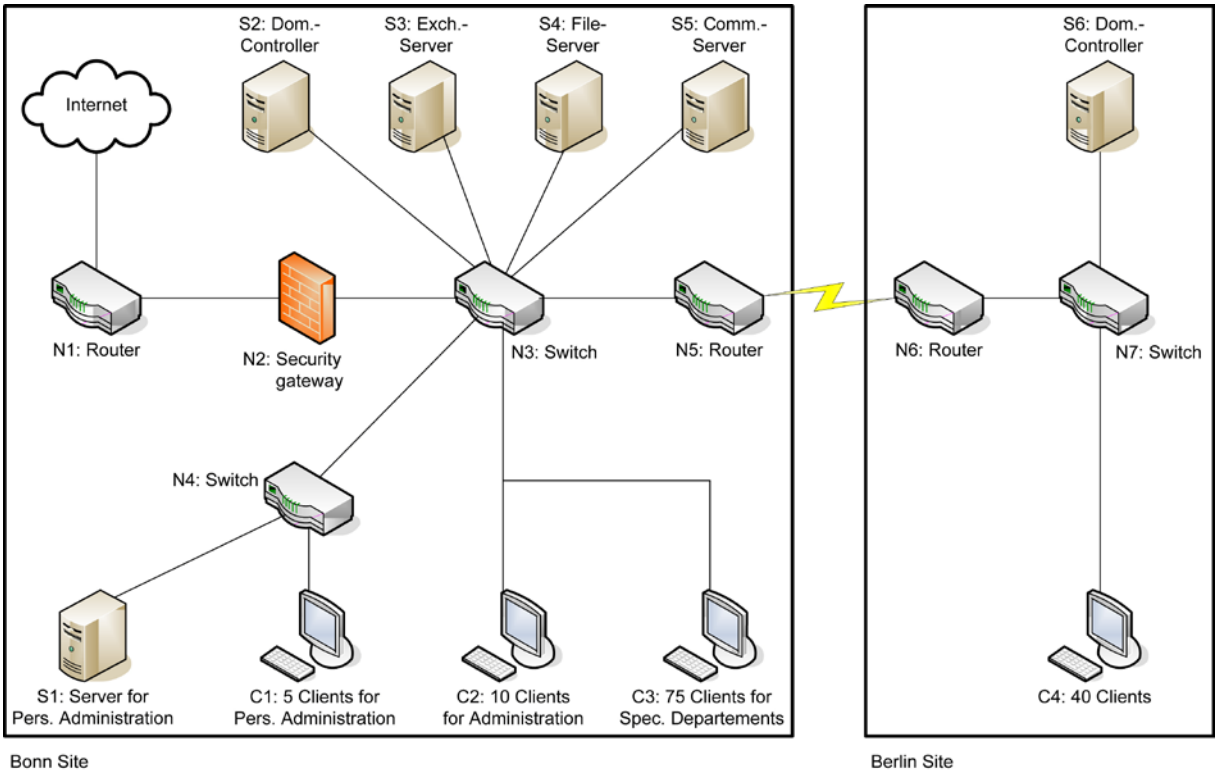


Figure 6: Example of a network plan created during the structure analysis

In the network plan shown, the IT systems are indicated by a number (i.e. *Sn, Cn, and Nn* for servers, clients, and active network components, respectively) together with its function.

The clients have been combined into suitable groups in Berlin and in Bonn. All 130 clients have virtually the same configuration, but there are differences between them in terms of the information they process, the applications, how they are integrated into the network, and their underlying infrastructure. Group C1 represents the 5 clients in the Personnel Department. They have access to Server S1 in the Personnel Department in Bonn. C2 and C3 represent the 10 clients in the Administration Department and the 75 clients in the specialised departments in Bonn. The only differences between them are the application programs they use. Finally, group C4 represents the clients in the specialised departments in Berlin. These differ from groups C1 to C3 in terms of their surrounding infrastructure and their integration into the overall network.

Action Points for 4.2.3 Preparing a network plan:

- Examine any existing graphic diagrams of the network, for example the network topology plans
- If necessary, update the existing network plans or create new ones
- Examine the additional information available on the IT systems contained and update and complete, if necessary
- Examine the additional information available on the communication links contained and update and complete, if necessary

4.2.4 Survey of the IT Systems

Keeping in mind that the protection requirements and information domain modelling will need to be performed later, a list of the existing and planned IT systems should be produced in the form of a table. The term "IT assets" not only refers to computer but also to active network components, network printers, telecommunication systems, etc. The focus is on the technical implementation of an IT system, for example if it is a workstation PC, Windows Server 2003, Windows XP client, Unix

server, telecommunications system, etc. At this point, only the system as such should be considered (e.g. Unix servers) and not the individual components making up the corresponding IT system (i.e. computer, keyboard, monitor, etc.).

Complete and correct documentation of the existing and planned IT systems is not only used to create a security concept. It is also required for checking, maintaining, trouble-shooting, and repairing IT systems.

Both the networked and non-networked IT systems are to be documented, especially those systems not previously incorporated into the network plan. IT systems which have been grouped together in the network plan can still be handled as a single object, though. Even IT systems not listed in the network plan must be checked to see if they can be assigned to an appropriate group. This may be possible, for example, for a large number of stand-alone workstation PCs that meet the requirements in the section 4.2.1 for forming groups and can therefore be grouped together.

When collecting the data, the following information, which will be needed in later stages, should be noted:

- A unique name for the IT system
- A description (type and function)
- The platform (e.g. hardware architecture/operating system)
- In the case of groups, the number of IT systems grouped together
- The installation site of the IT-system
- The status of the IT system (operational, test phase, in planning)
- Users and administrators of the IT system

After that, the applications are assigned to those IT systems which are needed to run them. These systems could be the IT systems on which the applications are processed, but they could also include systems that transfer data generated by the applications. The result is an overview that illustrates the relationships between the most important applications and the corresponding IT systems.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 3

As an example, the following table shows an excerpt from the list of IT systems in the BOV. A complete list can be found among the resources for IT-Grundschutz on the BSI web site.

No.	Description	Platform	Number	Installation Site	Status	Users
S1	Server for personnel administration	Windows Server 2003	1	Bonn, R 1.01	Operational	Personnel Department
S2	Domain controller	Windows Server 2003	1	Bonn, R 3.10	Operational	All IT users
C1	Group of clients in personnel data processing	Windows Vista	5	Bonn, R 1.02 - R 1.06	Operational	Personnel Department
C2	Group of clients in the Administration Department	Windows Vista	10	Bonn, R 1.07 - R 1.16	Operational	Administration Department
C6	Group of laptops for the Berlin office	Laptop running Windows Vista	2	Berlin, R 2.01	Operational	All IT users in the Berlin

No.	Description	Platform	Number	Installation Site	Status	Users
						branch office
N1	Router for Internet access	Router	1	Bonn, R 3.09	Operational	All IT users
N2	Firewall	Application gateway on Unix	1	Bonn, R 3.09	Operational	All IT users
N3	Switch	Switch	1	Bonn, R 3.09	Operational	All IT users
T1	Telecommunications system for Bonn	ISDN system	1	Bonn, B.02	Operational	All employees in the Bonn main office

The IT systems/groups S1, S2, C1, C2, N1, N2, and N3 are taken directly from the network plan. In addition, the non-networked IT system groups C6 (laptops) and T1 (telecommunication systems) have been added.

The following contains an excerpt of the application assignments to the affected IT systems for the fictitious BOV agency:

Description of the applications		IT systems						
No.	Application / Information	S1	S2	S3	S4	S5	S6	S7
A1	Processing of personnel data	X						
A2	Benefits processing	X						
A3	Travel expense accounting	X						
A4	User authentication		X				X	
A5	System management		X					
A6	Office communication			X				
A7	Central document administration				X			
A8	USB sticks for use when exchanging data media							

Key: Ai X Sj = The execution of IT application Ai depends on IT system Sj.

Action Points for 4.2.4 Survey of the IT Systems

- Check if the existing databases or overviews of the existing or planned IT systems are suitable for use as the starting point for the further procedures
- Create or update and complete the list of networked and non-networked IT systems
- Assign the IT systems or IT system groups a unique name or code
- Assign the applications to the IT systems (servers, clients, network switching elements, etc.) that are required for their execution

4.2.5 Documenting the rooms

The business processes and specialised tasks examined are not only operated on the defined IT systems, but are also located within the limits of the organisation's geographical infrastructure. Depending on the size of the organisation and many other factors, an organisation may be located in its own building or just on one floor of a building. Many organisations also use properties separated by great distances or that have to be shared with other users. In many cases, the business processes and specialised tasks are also executed in external premises, for example in the context of service contracts.

All properties on which the business processes and specialised tasks are executed must be included in a security concept. This includes the organisation’s premises, buildings, floors, rooms, and the routes between them. All communication links running through properties that are accessible to third parties must be handled as external communication links. This also applies to wireless communication connections if it cannot be guaranteed that it is impossible for third parties to obtain access to these networks.

For the further modelling procedure based on IT-Grundschutz and for planning the target/actual comparison, it is useful to produce an overview of all properties, and especially of the rooms in which the IT systems are located or which are used for IT operations. This includes rooms used exclusively for IT operations (such as server rooms and data media archives) and those in which, among other things, IT systems are operated (such as offices), but also the routes used for the communication links. If IT systems are placed in a protective cabinet instead of a special technical room, then the cabinet is to be documented just like a room.

Note: When documenting the IT systems, the installation location should have already been recorded.

In addition, it must be checked if information requiring protection is also stored in any other rooms. If this is the case, then these rooms must also be documented. Rooms in which non-electronic information requiring protection is stored, meaning document files or microfilms, must also be documented in this case. The type of information processed must be clear according to this documentation.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 4

The following excerpt shows how an overview of the rooms could appear for the fictitious BOV agency. There is already space to define the protection requirements of the rooms, but these columns are first filled out in a later step.

Room			IT / Information	Protection requirements		
Name	Type	Location	IT systems / data media	Confidentiality	Integrity	Availability
R U.02	Data Media Archives	Bonn building	Backup data media (weekly backups of servers S1 to S5)			
R B.02	Technology room	Bonn building	Telecommunications system			
R 1.01	Server room	Bonn building	S1, N4			
R 1.02 - R 1.06	Offices	Bonn building	C1			
R 3.11	Protective cabinet in room	Bonn building	Backup data media (daily backups of			

Room			IT / Information	Protection requirements		
	R 3.11		servers S1 to S5)			
R E.03	Server room	Berlin building	S6, N6, N7			
R 2.01 - R 2.40	Offices	Berlin building	C4, some with fax machines			

Action Points for 4.2.4 Documenting the Rooms
▪ Create a list of all properties, buildings, and rooms when documenting the IT systems
▪ Add any other rooms in which information requiring protection or processed in some other manner is stored to the list

4.3 Determining the protection requirements

The goal of defining the protection requirements is to decide for each object documented in the information domain which protection requirements the object has in terms of confidentiality, integrity and availability. These protection requirements are based on the potential damage which comes in conjunction with the impairment of the affected applications and therefore of the corresponding business processes.

The protection requirements are defined for the information domain in several steps:

- Definition of the protection requirement categories
- Determination of the protection requirements for applications
- Determination of the protection requirements for IT systems
- Determination of the protection requirements for rooms
- Determination of the protection requirements for communications links
- Conclusions drawn from the results of the protection requirements determination

After defining the protection requirements categories, the protection requirements for business processes and applications are then defined based on the typical damage scenarios. After that, the protection requirements for each IT system, room, and communication link are then derived from the results.

This procedure is described in more detail in the following sections.

4.3.1. Defining the protection requirements categories

Since the protection requirements are not usually quantifiable, IT-Grundschutz restricts itself to providing a qualitative statement by dividing the protection requirements into three categories:

Protection Requirements Categories	
"Normal"	The impact of any loss or damage is limited and calculable.
"High"	The impact of any loss or damage may be considerable.
"Very High"	The impact of any loss or damage may be of catastrophic proportions which could threaten the very survival of the organisation.

The following steps describe how to determine the appropriate protection requirements category for business processes and their underlying applications.

The damage that could occur if the confidentiality, integrity, or availability is lost for a particular business process or application, including its data, can usually be categorised according to the following damage scenarios:

- Violations of laws, regulations, or contracts
- Impairment of the right to informational self-determination
- Physical injury
- Impaired ability to perform the tasks at hand
- Negative internal or external effects
- Financial consequences

Frequently, several damage scenarios will apply to a single damage event. For example, the failure of an application could prevent essential work from being performed, resulting in direct financial loss and, at the same time, in a tarnished reputation.

In order to differentiate between the "normal", "high", and "very high" protection requirements categories, it may be appropriate to determine the limits of each damage scenario. The following tables are used to determine the protection requirements resulting from a potential damage scenario and its consequences. Each organisation must adapt the tables to reflect its own situation.

Protection requirements category "Normal"	
1. Violations of laws, regulations, or contracts	▪ Violations of regulations and laws with minor consequences ▪ Minor breaches of contract which result in at most minor contractual penalties
2. Impairment of the right to informational self-determination	▪ This deals with personal data whose processing could adversely affect the social standing or financial well-being of those concerned.
3. Physical injury	▪ Does not appear possible.
4. Impaired ability to perform tasks	▪ Impairment was assessed to be tolerable by those concerned. ▪ The maximum acceptable downtime is greater than 24 hours.
5. Negative internal or external effects	▪ Only minimal impairment or only internal impairment of the reputation / trustworthiness of the organisation is expected.
6. Financial consequences	▪ The financial loss is acceptable to the organisation.

Protection requirements category "High"	
1. Violation of laws, regulations or contracts	▪ Violations of regulations and laws with substantial consequences ▪ Major breaches of contract with high contractual penalties
2. Impairment of the right to informational self-determination	▪ This aspect deals with personal data whose processing could have a seriously adverse affect on the social standing or financial well-being of those concerned.
3. Physical injury	▪ Physical injury to an individual cannot be absolutely ruled out.
4. Impaired ability to perform tasks	▪ Impairment of the ability to perform the tasks at hand was assessed as intolerable by some of the individuals concerned. ▪ The maximum acceptable down time is between one and 24 hours.
5. Negative internal or external effects	▪ Considerable impairment of the reputation / trustworthiness can be expected.
6. Financial consequences	▪ The financial loss is considerable, but does not threaten the existence of the organisation.

Protection requirements category "Very high"	
1. Violation of laws, regulations or contracts	▪ Fundamental violations of regulations and laws ▪ Breaches of contract with ruinous damage liabilities
2. Impairment of the right to informational self-determination	▪ This aspect deals with personal data whose processing could result in the injury or death of the persons concerned or that could endanger the personal freedom of the persons concerned.
3. Physical injury	▪ Serious injury to an individual is possible. ▪ There is a danger to life and limb.
4. Impaired ability to perform tasks	▪ Impairment of the ability to perform tasks was assessed as intolerable by all individuals concerned. ▪ The maximum acceptable down time is less than one hour.
5. Negative internal or external effects	▪ A nation-wide or state-wide loss of reputation / trustworthiness is conceivable, possibly even endangering the existence of the organisation.
6. Financial consequences	▪ The financial loss threatens the existence of the organisation.

If it is determined when examining an object that there may be other damage scenarios not covered by the given six scenarios, then these scenarios should be added to the table accordingly. It is also

necessary to specify where the limits are to be drawn between the "normal", "high", and "very high" categories for all damage scenarios that do not fit into these scenarios.

Furthermore, the individual circumstances of the organisation should be taken into account. A loss of €200,000 could be relatively trivial when compared to the sales volume and IT budget in a large company, but even a loss of €10,000 could threaten the existence of a small organisation. It may therefore be appropriate to express the limits as percentages of total sales, total profit, or on a similar base value.

Similar considerations could be employed in terms of the availability requirements. For example, a downtime of 24 hours could still be regarded as acceptable for the "normal" protection requirement category in some organisations. If these failures occur often, for example more than once a week, then the total downtime may not be tolerable. The availability requirements specified based on the protection categories should therefore be specified in detail when necessary.

To estimate the protection requirement for the "Impairment of the right to informational self-determination", there are specific examples available from several German state data protection officers which are explained using protection level concepts.

When specifying the limit between "normal" and "high", the fact that the IT-Grundschutz standard security safeguards should be adequate for normal protection requirements should be taken into account. The specifications made must be appropriately documented in the security concept because the selection of security safeguards, and therefore the subsequent cost, depends on this.

Action Points for 4.3.1 Defining the protection requirements categories
▪ Examine typical damage scenarios to define the protection requirements categories
▪ Define the "normal", "high", and "very high" protection requirements categories, or adapt them accordingly to the organisation

4.3.2 Determination of the protection requirements for applications

Based on the possibility that the confidentiality, integrity, or availability of an application or the corresponding information could be lost, the maximum and subsequent damage that could arise from such a situation is examined. By answering the question "What would happen if ...?", realistic damage scenarios are developed *from the user's point of view*, and the expected material or non-material damage is described. The extent of this possible damage ultimately determines the protection requirement of the application. It is essential in this case for the person responsible for the application being examined and its users are asked for their own personal assessment. They usually have a good idea of what damage could occur and should be able to provide useful information to help determine the protection requirements.

The data media and document groups documented during the structure analysis must also be included when determining the protection requirements.

To simplify the determination of the possible damage and its effects, a set of questions is presented in the Appendix of this standard. These suggestions do not claim to be complete; they are merely intended as a guide. In any case, it is necessary to consider the specific tasks at hand and the situation of the organisation and adapt the questions provided in this manual or add new questions accordingly.

The specification of the protection requirement for the application being examined is a decision relating to risk management which often has far-ranging consequences for the security concept for the information domain being examined. The protection requirements for the applications are integrated into the protection requirements specifications of the affected technical and infrastructural objects, such as for the servers and rooms.

In order to be able to understand the results of the protection requirements determination and the reasons for the decision made later on in the context of information security management based on

these requirements, the results of the protection requirements determination for the applications must be well-documented. Care should be taken here to ensure that not only are the protection requirement specifications documented, but the corresponding reasons for these decisions are provided. Providing reasons will ensure that others will be able to check the specifications later and reuse them if possible.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 5

The following table shows the main applications, their protection requirements, and the reasons for selecting the given protection requirement for the fictitious BOV agency.

Application			Protection requirements		
No.	Name	Pers. data	Basic Value	Protection requirements	Reasons
A1	Processing of personnel data	X	Confidentiality	High	Personal data consists of particularly sensitive personal data whose disclosure could significantly harm the person concerned.
			Integrity	Normal	The protection requirements are normal since errors are detected quickly and the data can be corrected later on.
			Availability	Normal	Downtimes of up to one week can be overcome by following manual procedures.
A2	Benefits processing	X	Confidentiality	High	Benefits data includes personal data which has particularly high protection requirements and which may contain information on illnesses or medical test results. Disclosure of this data could be very harmful to the persons concerned.
			Integrity	Normal	Protection requirements are normal as errors are detected quickly and the data can be corrected later.
			Availability	Normal	Downtimes of up to a week can be handled by following manual procedures.

At this point, it may be appropriate to look beyond this information and consider the protection requirements from an overall perspective of the business processes or specialised tasks. It is appropriate in this case to describe the purpose of an application in a business process or a specialised task and to derive its importance based on its purpose. This importance can be classified as follows:

The importance of the application for the business process or specialised task is:

- **Normal:** The business process or specialised task can be performed by alternative means (e.g. manually) at a level of additional expense that is acceptable

- **High:** The business process or specialised task can only be performed by alternative means (e.g. manually) at significant additional expense
- **Very high:** The business process or specialised task cannot be performed at all without the application

In particular, the advantage of undertaking such an overall perspective is that management can act as a regulator for the protection requirements for the individual applications when defining the protection requirements. For example, it may be that a person responsible for an application views its protection requirements as "normal", whereas management might estimate it to be more important due to its perspective of the business process or specialised task.

This optional information should also be documented in a table or with the help of the corresponding software products.

Action Points for 4.3.2 Determination of the protection requirements for applications
▪ Determine the protection requirements for the documented applications based on the damage scenarios and catalogue of questions ▪ Document the protection requirements of the applications and the reasons for the requirements in tables

4.3.3 Determining the protection requirements for IT systems

In order to determine the protection requirements of an IT system, the applications related directly to the IT system must be examined first. An overview of which applications are relevant for the various IT systems was created in conjunction with the structure analysis (see section 4.2.4). The protection requirements of the application (see section 4.3.2) are integrated into the protection requirement definition for the correspondingly affected IT systems.

To determine the protection requirements of the IT system, the total potential damage to the relevant applications must be considered. The damage event or total damage with the most serious consequences determines the protection requirements of an IT system (**maximum principle**).

When examining the possible damage and its consequences, it must also be kept in mind that the applications may use the results of other applications as input. A seemingly unimportant application A can assume significantly greater importance if another, more important application B depends on its results. In this case, the protection requirements determined for application B must also be assigned to application A. If these applications are on different IT systems, then the protection requirements of the one IT system must be assigned to the other IT system (**accounting for dependencies**)

If several applications or a lot of information is processed on an IT system, then you must determine if the accumulation of several (e.g. smaller) damage events on one IT system could result in a higher amount of total damage. In this case, the protection requirements of the IT system increase accordingly **(cumulative effect)**.

Example: All applications required for recording customer data in an organisation are located on one network server. The damage in the event of the failure of this application was estimated to be low since there are enough possible alternatives. However, if the server fails (and therefore all the applications as well), then the estimate of the resulting damage must be assessed considerably higher. The organisation may possibly no longer be able to perform its tasks within the required time frame under some circumstances. For this reason, the estimated protection requirements of these "central" components should also be higher.

The opposite effect can also occur. This means it is possible for an application to have high protection requirements, but its protection requirements are not assigned to the IT system being examined because only minor parts of the application run on that IT system. In this case, the protection requirements have to be reallocated (**distribution effect**).

Examples: The distribution effect occurs mainly for the basic value of availability. For example, when IT systems have been designed to be redundant, the protection requirements of the individual components may be lower than the protection requirement of the entire application. Distribution effects are also possible in terms of the confidentiality: If it is ensured that a client can only call

uncritical data from a highly confidential database application, then the client may have lower protection requirements than the database server under some circumstances.

Presentation of the results

The results of the protection requirements determination for the IT systems should be documented in a table. This table should also indicate the protection requirements for every IT system in terms of the confidentiality, integrity, and availability. The overall protection requirements of an IT system are in turn derived from the maximum protection requirements for the three basic values of confidentiality, integrity, and availability. Therefore, an IT system has high protection requirements when one or more of the basic values have a "high" protection requirement. However, it is generally advisable to document the protection requirements of an IT system for all three basic values separately because different types of security safeguards usually result from this separation.

For an IT system, for example, the overall protection requirement may be high because the confidentiality protection requirement is high even though the protection requirements are normal for the integrity and availability. In this case, the overall protection requirements are specified to be high, but this does not imply that the protection requirements for integrity and availability have to be raised as a result.

The specifications of the protection requirements of the IT systems must be justified so that the decisions made can be understood by persons not participating in the protection requirement determination. In this case, you can refer to the protection requirements of the applications.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 6

The results of the protection requirements determination for the IT systems should be documented as follows in a table (sample excerpt).

IT System		Protection requirements		
No.	Description	Basic Value	Protection requirements	Reasons
S1	Server for personnel administration	Confidentiality	High	Maximum principle
		Integrity	Normal	Maximum principle
		Availability	Normal	Maximum principle
S2	Domain controller	Confidentiality	Normal	Maximum principle

IT System		Protection requirements		
		Integrity	High	Maximum principle
		Availability	Normal	Due to the protection requirement specification for application A4, the protection requirement for this basic value can be assumed to be high. However, it should be kept in mind that this application is distributed between two computer systems. It is also possible for employees working in the Bonn office to be authenticated via the second domain controller S6 in Berlin. A failure of domain controller S2 is acceptable for a period of up to 72 hours. Therefore, the protection requirement is "normal" as a result of distribution effects.

Note: If most applications on an IT system only have normal protection requirements and only one or a few applications have high protection requirements, then consideration should be given to transferring these applications to an isolated IT system since it is much easier, and therefore often less expensive, to secure them on an isolated IT system. This alternative can be submitted to management, who then decides which alternative to use.

Action Points for 4.3.3 Determining the protection requirements for IT systems

- Determine the protection requirements of the IT systems based on the protection requirements of the applications
- Take any dependencies, the maximum principle, and if necessary the cumulative or distribution effects into account
- Document the results for the confidentiality, integrity, and availability as well as the reasons for the decisions for each IT system (group)

4.3.4 Determining the protection requirements for rooms

The protection requirements for the buildings and rooms should be derived from the results of the protection requirements determination for the corresponding applications and IT systems. These protection requirements are derived from the protection requirements for the IT systems installed in the relevant room, the information they process, or the data media stored and used in the room according to the maximum principle. When deriving the protection requirements, any dependencies and possible cumulative effects should be taken into account when there are a large number of IT systems located in a room, which is typically the case for server rooms, computer centres, and data media archives. The reasons for the estimated protection requirements should be documented.

Documenting the necessary information in tables based on the overview of documented rooms created earlier.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 7

The following table shows an excerpt of the results of the protection requirements determination for the rooms of the fictitious BOV agency.

Room			IT / Information	Protection requirements		
Name	Type	Location	IT systems / data media	Confidentiality	Integrity	Availability
R U.02	Data media archives	Bonn building	Backup data media (weekly backups of servers S1 to S5)	High	High	Normal
R B.02	Technology room	Bonn building	Telecommunications system	Normal	Normal	High
R 1.01	Server room	Bonn building	S1, N4	High	High	Normal
R 1.02 - R 1.06	Offices	Bonn building	C1	High	Normal	Normal
R 3.11	Protective cabinet in room R 3.11	Bonn building	Backup data media (daily backups of servers S1 to S5)	High	High	Normal
R E.03	Server room	Berlin building	S6, N6, N7	Normal	High	High
R 2.01 - R 2.40	Offices	Berlin building	C4, some with fax machines	Normal	Normal	Normal

Action Points for 4.3.4 Determining the protection requirements for rooms

- Derive the room's protection requirements from the protection requirements of the IT systems and applications
- Take any dependencies, the maximum principle, and if necessary the cumulative effects into account
- Document the results and reasons so that they can be understood by someone else

4.3.5 Determining the protection requirements for communications links

Once the determination of the protection requirements for the applications, IT systems, and rooms being examined has been completed, the protection requirements for the networking structure must be determined. The basic information required for these considerations can be found in the network plan created in section 4.2.3 for the information domain under examination.

The communications links must now be analysed to provide a basis for the decisions regarding which communication routes require the use of cryptographic security safeguards, which sections of the network should be designed redundantly, and which connections are expected to be used in attacks by internal and external perpetrators. In this analysis, the following communications links should be regarded as critical:

- Communication links to the outside world, i.e. which lead into or through uncontrolled areas (for example into the Internet or over property that can be accessed by the general public). These communication links could also include WLAN connections because it is difficult to prevent access to them from public property. For external connections, there is a risk that external attackers could attempt to penetrate the system to be protected or that computer viruses or Trojan horses could be imported. Furthermore, an insider could pass confidential information to the outside world over such connections under certain circumstances. The basic value of availability is also often threatened in particular by communication links to the outside world

- Communications links which are used to transmit information with high protection requirements. The information in this case could be information with a high confidentially, integrity, or availability requirement. These links could be targeted for deliberate attempts to listen in on the communication or manipulate data. In addition, the failure of such a link could have an adverse effect on the operational capability of a large part of the information domain.
- Communications links which may not be used to transmit certain highly sensitive information. In this case, the primary concern is the transmission of confidential information. For example, if there are any network switching elements that are inappropriately or incorrectly configured, it could be possible for precisely the information which is not permitted to be transmitted over such connections to be transmitted nevertheless, and the information is therefore vulnerable to attack.

One approach to determining which communications links are critical is as follows. First, all "external connections" are identified and documented to be critical connections. After that, all links that are used by IT systems with high or very high protection requirements are examined. In this examination, the connections used to transit information with high protection requirements are identified. Subsequently, the connections further downstream which are used to transfer this highly sensitive data are examined. Finally, the communication links which must not be allowed to be used to transmit such information are identified. The information documented should include:

- The communications routes
- Whether or not the connection has a link to the outside world
- If information having high protection requirements is transmitted and if this protection requirement results from the required confidentiality, integrity, or availability
- If information having high protection requirements must not be allowed to be transmitted over the link
- The decision of which communication links are to be viewed as critical should be documented in a table or highlighted graphically in the network plan.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 8

In our fictitious example of the BOV, the following critical connections were found:

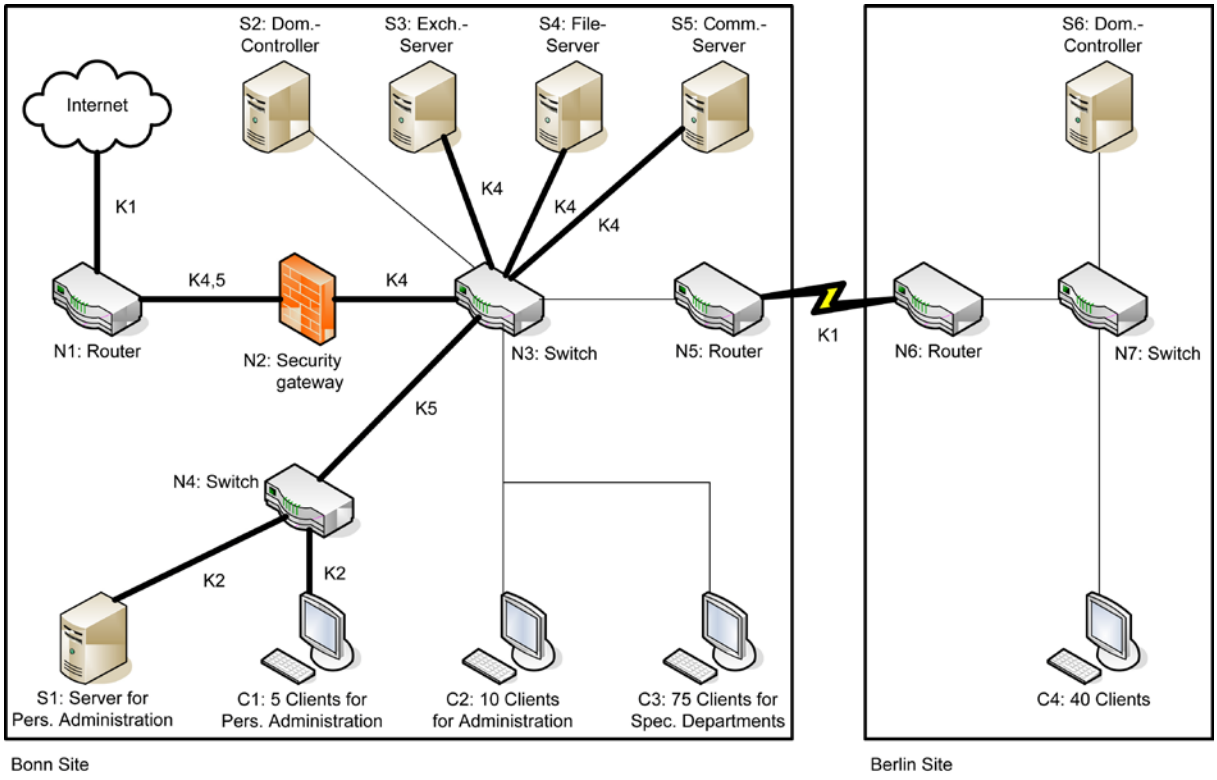


Figure 7: Example of a network plan with critical connections

In the diagram, the critical connections are indicated by the thick lines. The numbers after the letter "C" in the codes next to the lines indicate the reason(s) why the corresponding connection is critical. The codes are explained in the column headings in the following table.

	Critical because				
Connection	K 1 Outside connection	K 2 Highly Confidential	K 2 High Integrity	K 2 High Availability	K 5 Transmission not permitted
N1 - Internet	X				
N5 - N6	X				
S1 - N4		X			
S3 - N3				X	
S4 - N3				X	
S5 - N3				X	
C1 - N4		X			
N1 - N2				X	X
N2 - N3				X	
N4 - N3					X

When creating this table, particular care should be taken to ensure that the overview produced is complete. Overlooking just **one** critical connection can undermine the overall security. Outside connections can be established through dedicated connections, DSL access points, fax connections, wireless networks, and ISDN interfaces, for example. Many modern laptops have integrated interfaces for modem and wireless connection. All-in-one devices that can be used for scanning, copying, and

printing often have a built-in modem to provide faxing capabilities. If communication paths such as these or similar to these are used, then these paths must be integrated systematically into the security process.

Action Points for 4.3.5 Determining the protection requirements for communication links
▪ Document the external connections ▪ Identify all connections that are used to transfer critical information ▪ Determine which communication links must not be used to transmit certain information ▪ Document all critical communication links in the form of a table or graph

4.3.6 Conclusions drawn from the results of the protection requirements determination

The results obtained from the protection requirements determination provide a starting point for the further development of the security concept. The following is assumed for protection requirements categories encompassing protection going beyond the standard security safeguards recommended by IT-Grundschutz:

Protective effect of standard security safeguards in IT-Grundschutz	
"Normal" protection requirements category	Standard IT-Grundschutz security safeguards are generally adequate and appropriate.
"High" protection requirements category	Standard IT-Grundschutz security safeguards provide a basic level of protection but may not be sufficient alone under some circumstances. Additional safeguards can be determined by performing a supplementary security analysis.
"Very high" protection requirements category	Standard IT-Grundschutz security safeguards provide a basic level of protection but are generally not sufficient on their own. The required additional safeguards must be determined individually on the basis of a supplementary security analysis.

In addition to when the protection requirement is high or very high, a supplementary security analysis must also be performed when the following applies to the objects in the information domain under examination:

- The objects could not be adequately depicted (modelled) with the existing IT-Grundschutz modules
- The objects are used in operating scenarios (environment, application) that are not mentioned in IT-Grundschutz

You will find more detailed information on the supplementary security analysis in section 4.6.

Areas with varying protection requirements

When determining the protection requirements, it is often the case that there are areas in the information domains being examined in which information with high or very high protection requirements is processed. Even if only a few specific data items have higher protection requirements, the high level of networking and interlinking of IT systems and applications rapidly leads to the requirement for higher protection for other areas due to the maximum principle.

Therefore, security zones with different security levels should be set up to minimise risks and costs. Such security zones could be based on rooms, technology, or personnel.

Examples:

- Geographical security zones: So that it is not necessary to permanently lock or monitor every single office, zones having a lot of visitors should be separated from areas that have high protection requirements. Therefore, meeting, training, and event rooms as well as the canteen (which attracts external customers) should be located near the entrance to the building. A gatekeeper could then easily monitor access to the part of the building containing the offices. Particularly sensitive areas such as a development department should have additional access control, for example using chip cards.
- Technical security zones: In order to restrict confidential data to certain areas in a LAN, to prevent malfunctions from affecting certain components, and to prevent attacks on the operability, it is helpful to divide the LAN into several sub-networks (refer also to S 5.77 Establishing sub-networks in the IT-Grundschutz Catalogues).
- Personnel security zones: Basically, each person should only be assigned the rights required to perform their tasks. In addition, there are also various roles that should not be assumed by one and the same person. For example, an auditor should not work in bookkeeping or in IT administration at the same time since he should not and cannot be allowed to audit himself. In order to simplify the assignment of access rights, groups of people who perform functions that lead to conflicts of interest should work in different groups or departments.

When planning new business processes, specialised tasks, or applications, it should be examined early if it makes sense to establish security zones. This can often save a lot of work in all subsequent phases, even up to the auditing phase.

Action Points for 4.3.6 Conclusions drawn from the results of the protection requirements determination
▪ Check if objects with increased security requirements can be concentrated in security zones ▪ Mark all objects with higher security requirements for a supplementary security analysis

4.4 Selecting and adapting safeguards

Once the required information is available from the structure analysis and the protection requirements have been determined, the next major task is to model the information domain under examination with the help of the modules available in the IT-Grundschutz Catalogues. The result is an IT-Grundschutz model for the information domain consisting of a variety of modules, some of which may be used a number of times, and which maps the modules to the security-related aspects of the information domain.

4.4.1 The IT-Grundschutz Catalogues

The current version of the IT-Grundschutz Catalogues [GSC] can be downloaded from the BSI web server.

Modules

The IT-Grundschutz Catalogues contain the threat scenarios and the recommended safeguards for various components, procedures, and IT systems, which are then consolidated into one module for each subject.

Every module begins with a description of the typical threat scenarios to be expected in the given area together with their overall probability of occurrence. Each threat scenario is part of a simplified risk analysis for typical information processing environments and forms the basis for the specific bundle of safeguards developed by BSI for the areas of infrastructure, personnel, organisation, hardware and

software, communication, and contingency planning. The advantage of this is that the users are not required to perform complex analyses to reach the security level required for average protection requirements. Instead, it is sufficient in this case to identify the modules relevant to the IT systems or business processes being examined and to implement the recommended safeguards thoroughly and completely. Even if there are special components or operating environments that are not adequately discussed in IT-Grundschutz, the IT-Grundschutz Catalogues is still a valuable tool. The necessary supplementary security analysis can concentrate on the specific threats to these components or environmental conditions.

To take the surges in innovation and version changes in the IT industry into account properly, the IT-Grundschutz Catalogues are organised into modules and can therefore be expanded and updated easily.

The modules are grouped into the following chapters:

1: General aspects

2: Infrastructure

3: IT systems

4: Networks

5: Applications

Threat Catalogues

This section contains detailed descriptions of the threats that are included in the threat scenarios for the individual modules. The threats are grouped into five catalogues:

T 1: Force majeure

T 2: Organisational shortcomings

T 3: Human error

T 4: Technical failure

T 5: Deliberate acts

Safeguard Catalogues

This part describes the safeguards mentioned in the modules of the IT-Grundschutz Catalogue in detail. The safeguards are grouped into six catalogues:

S 1: Infrastructure

S 2: Organisation

S 3: Personnel

S 4: Hardware and software

S 5: Communication

S 6: Contingency planning

4.4.2 Modelling and information domain

It makes no difference to the IT-Grundschutz model created whether the information domain consists of IT systems already in operation or the information domain in question is still in the planning stage. However, the model can be used for different purposes:

- The IT-Grundschutz model for an information domain already in operation identifies the relevant standard security safeguards using the selected modules. It can be used in the form of a **test plan** to compare the current state to the target state.

- In contrast, the IT-Grundschutz model for an information domain in planning represents a **development concept**. Using the selected modules, it described which standard security safeguards must be implemented when the information domain is in operation.

The diagram below illustrates the role of modelling and its possible results:

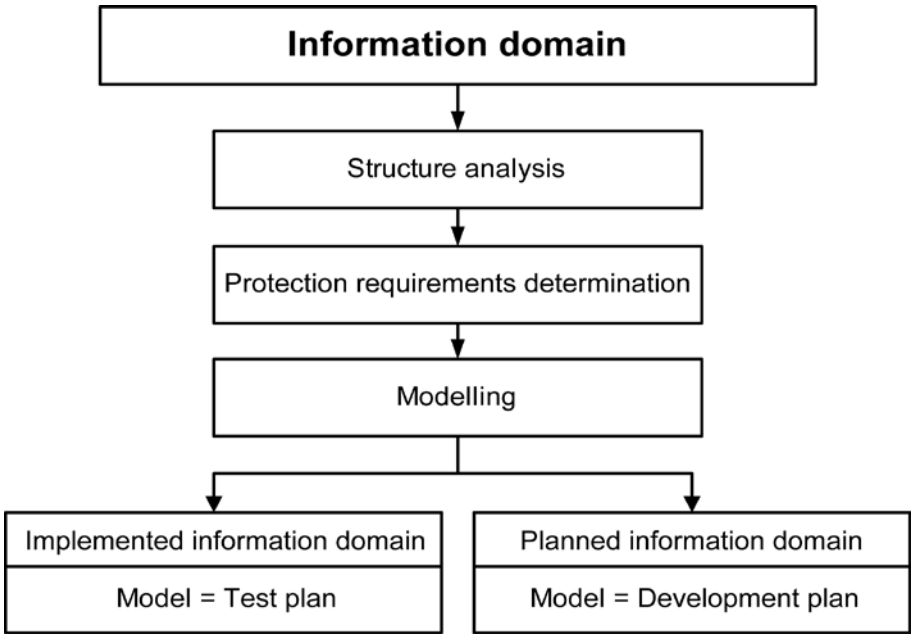


Figure 8: Results of modelling according to IT-Grundschutz

Typically, an information domain currently in operation will not only contain parts that have already been implemented, but also parts which are still in the planning stage. The resulting IT-Grundschutz model then contains both a test plan and some elements of a development concept. The security safeguards envisioned in the test plan or development concept then form the basis for the development of the security concept. In addition to the security safeguards already implemented that were identified as inadequate or missing during the current/target state comparison, this also includes the safeguards for the parts of the information domain still in planning.

In order to portray information domains, which are usually complex systems, using the IT-Grundschutz modules, it is recommended to view the security aspects grouped according to certain subjects.

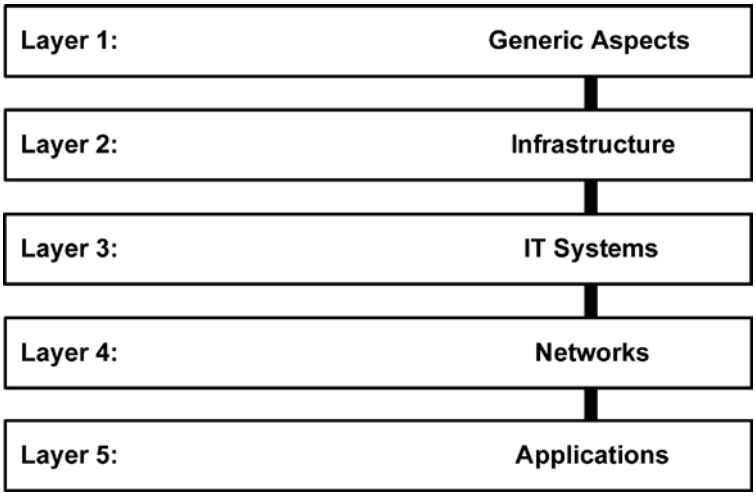


Figure 9: Layers in the IT-Grundschutz model

The security aspects of an information domain are assigned to the individual layers as follows:

- Layer 1 comprises the generic security aspects that apply to the entire information domain or a large part of it. This layer affects in particular the generic concepts and the regulations derived from the concepts. Typical Layer 1 modules include, among others, the *Security management, Organisation, Data Backup Policy,* and *Computer Virus Protection Concept* modules.
- Layer 2 deals with the architectural and structural conditions in which different aspects of infrastructural security come together. This layer affects in particular to the *Building, Server room, Protective cabinet,* and *Workplace at home* modules.
- Layer 3 deals with the individual IT systems in the information domain that have been grouped together, if necessary. This layer handles the security issues of clients, servers, and stand-alone systems. This layer includes, for example, the *Telecommunication system, Laptop,* and *Client using Windows XP* modules.
- Layer 4 examines the networking aspects not related to specific IT systems, but to the network links and communication. These include, for example, the *Heterogeneous networks, WLAN,* and *Remote access* modules.
- Finally, Layer 5 deals with the actual applications used in the information domain. This layer could include, among others, the *E-mail, Web server, Fax server* and *Databases* for modelling modules.

Using this layer approach has the following advantages.

- The level of complexity of the information security is reduced because the individual aspects are divided up in a meaningful manner.
- Since higher-level aspects and common infrastructural questions are examined separately from the IT systems, duplicated work is avoided because these aspects only need to be handled one time only and not once for every IT system.
- The individual layers have been selected so that the responsibilities for the aspects being examined are bundled. Layer 1 is concerned primarily with fundamental questions relating to the handling of information, Layer 2 with the building services, Layer 3 with the level of administrators and IT users, Layer 4 with the network and system administrators, and Layer 5 with those responsible for the applications and its users.
- Since the security aspects are divided into layers, individual subject areas in the resulting security concepts can be more easily updated and expanded without significantly affecting the other layers.

IT-Grundschutz modelling now consists of deciding if and how the modules in each layer can be used to model the information domain. Depending on the module being examined, the target objects of this model may be of different types: individual business processes or components, groups of components, buildings, properties, organisational units, etc.

The IT-Grundschutz model, i.e. the model of the module to target object assignments, should be documented in the form of a table containing the following columns:

- Number and title of the module
- Target object or target group: This could be the identification number of a component or a group, or the name of a building or organisational unit, for example.
- Contact person: This column serves initially only as a placeholder. The contact person is not specified in the modelling phase, but during the planning phase for the comparison of the target/actual states in the basic security check.
- Notes: Incidental information and the reasoning behind the model can be documented in this column

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 9

The following table is an excerpt from the modelling phase performed for the fictitious BOV Department.

No.	Title of module	Target object / target group	Contact person	Notes
1.1	Organisation	Bonn site		The Organisation module must be worked through separately for the Bonn and Berlin sites since Berlin has its own organisational rules.
1.1	Organisation	Berlin site		
1.2	Personnel	Entire BOV		The BOV's central Personnel Department is located in Bonn.
2.5	Data Media Archives	R U.02 (Bonn)		The backup data media are stored in this room
3.203	Laptops	C5		The laptops in Bonn and Berlin are place in two groups, one for Bonn and one for Berlin.
3.203	Laptops	C6		
5.4	Web servers	S5		S5 acts as the server for the Intranet.
5.7	Databases	S5		A database is used on Server S5.

A detailed description of the procedure for modelling an information domain can be found in the "Layer model and modelling" section of the IT-Grundschutz Catalogues. Particular emphasis is placed on the factors used to decide when it is appropriate to use a given module and to which target objects it should be applied.

4.4.3 Adapting safeguards

In the modelling process, the modules of the IT-Grundschutz Catalogue were selected which need to be implemented for each of the target objects in the information domain being examined. The modules provide suggestions for security safeguards which are typically suitable and appropriate for the given types of components.

To create a security concept or perform an audit, each of the safeguards must be worked through. IT-Grundschutz safeguards are formulated generally enough so that they are applicable to the largest possible number of environments, but with enough detail in the descriptions of the safeguards so that they can aid in implementing the safeguards as well.

This also means, though, that the suggested safeguards must be adapted to the environment of the corresponding organisation. It may make sense, for example,

- to specify the safeguards with more detail, for example by adding technical details;
- to adapt the safeguards to more accurately reflect the terminology used in the organisation, for example by changing the names of the roles; and
- to ignore any recommendations in safeguards which are not applicable to the area being examined.

In general, the basic ideas in the text of the safeguard should always be implemented. All changes to the recommendations in the IT-Grundschutz Catalogues should be documented so that the reasons for the changes can be understood later on as well.

To make adapting the IT-Grundschutz text to the corresponding target areas easier for the users, all text, modules, threats, safeguards, tables, and tools are also available in electronic form. This text can therefore be reused when creating a security concept and when implementing the safeguards.

When examining the safeguards, it may be the case that some of the suggested IT-Grundschutz safeguards are absolutely necessary under the given conditions. This could be the case, for example, when the corresponding threats can be counteracted with other, equivalent safeguards or the suggested safeguards are not applicable (because the corresponding service has not been activated, for example). Additional security safeguards and any safeguards ignored must be documented in the security concept. This also makes it easier to perform the basic security check.

When selecting and adapting the safeguards, it must always be ensured that the selections and changes are appropriate. Appropriate in this case means the following:

- Efficiency (Effectivity): The safeguards must provide effective protection against the possible threats, i.e. they must fulfil the security requirements identified.
- Suitability: It must be possible to actually implement the safeguards in practice, which means they may not impair the organisational procedures or bypass other security safeguards.
- Practicality: The safeguards should be easy to understand, easy to apply, and not prone to errors.
- Acceptance: All users must be able to use the safeguards (barrier-free) and must not discriminate against or adversely affect anyone.
- Efficiency: The best possible results should be attained with the resources used. On one hand, the safeguards should minimise the risk as much as possible, but the cost of implementation should remain in proper proportion to the value of the objects to be protected.

Action Points for 4.4 Selecting and adapting safeguards
▪ Systematically work through the "Layer model and modelling" section in the IT-Grundschutz Catalogues
▪ Determine which target objects in the information domain being examined applies to for each module in the IT-Grundschutz Catalogues
▪ Document the module to target object assignments ("IT-Grundschutz model") and the corresponding contact people
▪ Mark any target objects that could not be modelled properly for a supplementary security analysis
▪ Carefully read the text of each safeguard in the modules identified and adapt them accordingly, if necessary

4.5 Basic security check

The following considerations assume that the following parts of the security concept have already been created in accordance with IT-Grundschutz for the selected information domain.

Based on the structural analysis of the information domain, an overview of the existing IT equipment, where it is located, and the IT applications it supports was created. Based on this overview, the protection requirements were determined, the result of which was an overview of the protection requirements of the applications, IT systems, and rooms and communication links used. The information domain was modelled according to IT-Grundschutz with the help of this information. The result was a model of the information domain under examination based on the IT-Grundschutz modules.

This model based on IT-Grundschutz is now used as a test plan to determine which standard security safeguards have been implemented adequately and which inadequately by comparing the target state to the actual state.

This section describes how to proceed when performing the basic security check. This basic security check is performed in three different steps. The first step consists of making the organisational preparations and, in particular, selecting the relevant contact people for the target/actual state comparison. In Step 2, the target state is compared to the actual state by conducting interviews and performing random checks. In the final step, the results of the target/actual state comparison are documented together with the reasoning behind the results.

These three stages of the basic security check are described in detail in the following.

4.5.1 Organisational preparation for the basic security check

A certain amount of preliminary work is required to ensure that the target/actual state comparison proceeds smoothly. It is necessary to first inspect all the in-house documentation regulating the security-relevant processes, e.g. organisational instructions, work instructions, security instructions, manuals and "informal" procedures. These documents can be helpful in ascertaining the degree of implementation, especially for questions about existing organisational procedures. It is also necessary to clarify who is currently responsible for their contents in order to be able to determine who the correct contact person is later.

Next, it should be determined if and to what extent any external parties need to be involved in ascertaining the implementation status. This might be necessary, for example, for external computer centres, supervisory government agencies, companies which have outsourced some of the business processes or IT operations, or the building authorities responsible for infrastructural safeguards.

Another important step to be performed before actually comparing the target and actual states is to determine who it would be appropriate to interview. To do this, first specify a main contact person for every single module used to model the existing information domain.

- For the modules in "Higher order aspects of IT security" in Layer 1, a suitable contact person can generally be found directly in the corresponding subject section in the module. For example, for module 1.2 *Personnel*, the contact person should be an employee from the corresponding Personnel department. For the design modules, e.g. module 1.4 *Data Backup Policy*, it is best when the person who is responsible for updating the corresponding document is available as the contact person. Otherwise, the person whose tasks include updating the rules and regulations in the area under examination should be interviewed.
- For Layer 2, “Infrastructure", the selection of suitable contact persons should be co-ordinated with the departments providing general services and/or building services. Depending on the size of the organisation being examined, different contact persons could be responsible for the two “Building” and “Protective Cabinets” infrastructural areas, for example. In small organisations, the custodian will often be able to provide the information. It should be noted that external departments may need to participate in the area of infrastructure under some circumstances. This applies in particular to large organisations.
- In the modules in Layer 3 "IT systems" and Layer 4 "Networks", there is heavy emphasis on technical aspects in the security safeguards to be checked. This generally means that the main contact person will be the administrator for the component or group of components to which the module in question was assigned in the modelling phase.
- For the modules in Layer 5 "IT applications", the people who support or are responsible for the individual applications should be selected as the main contact persons.

In many cases, the main contact person will not be able to answer all questions on every aspect of the corresponding module. In this case, it is useful to interview one or more additional people to obtain more information. Information on who should be involved is provided in the "Initiation responsibility"

and "Implementation responsibility" entries found at the beginning of the description of every security safeguard.

A schedule should be created for the interviews with the system administrators, administrators, and other contact persons. Special attention should be given here to co-ordinating the appointments with people from other organisational units or other organisations. It also makes sense to agree on alternative dates for the interviews.

Depending on the size of the project team, the tasks should be divided between different interview teams, each of which with its own set of tasks. Experience has shown that using two-person teams works best. When interviewing, one person writes down the answers and comments to the questions while the other person asks the necessary questions.

Action Points for 4.5.1 Organisational preparation for the basic security check
▪ View all internal documents containing authorisations and regulations, and clarify who is responsible for these documents ▪ Determine to what extent assistance from external parties is required ▪ Stipulate a main contact person for every module used in the modelling phase ▪ Agree to appointments for interviews ▪ Assemble teams for the interviews

4.5.2 Performing the target/actual state comparison

Once all the necessary preliminary work has been completed, the actual analysis can start at the times specified beforehand. This includes working through the security safeguards contained in the module for which the person being interviewed is responsible one safeguard after another.

The following are possible answers to questions relating to the implementation status of individual safeguards:

"Unnecessary"	-	Implementation of the recommended safeguard is not necessary in the form suggested because other safeguards (e.g. safeguards not contained in IT-Grundschutz but which have the same effect) already provide sufficient protection against the corresponding threats, or because the safeguards recommended are not applicable (e.g. because certain services have not been activated).
"Yes"	-	All the recommendations in the safeguard have been fully, effectively, and properly implemented.
"Partially"	-	Some of the recommendations have been implemented, but others have not yet been implemented or only implemented in part.
"No"	-	Most of the recommendations contained in the safeguard have not been implemented yet.

It is not recommended to reading the text of the recommendations contained in a given safeguard out loud during the interview because the safeguard recommendations were not designed for interviewing purposes. For this reason, the interviewer needs to be familiar with the contents of the module, and a handy checklist with keywords should also be created for this purpose. In order to be able to clarify any disagreements in case of doubts, it is useful to have the full text of the safeguards nearby during the interview. However, it is not recommended to enter the answers directly into a PC during the interview since it would distract those involved and cause unwanted disruptions in communication.

Starting the interview with a few introductory words and a brief explanation of the purpose of the basic security check helps to create a relaxed, open, and productive working atmosphere. It would appear best to continue with the safeguard headings and briefly explain the safeguards. Rather than conducting a monologue, it is better to give the person being interviewed the opportunity to discuss those parts of the safeguard that have already been implemented and then to discuss any items that are still open.

The questions asked should always be concerned at first with the standard level of security safeguards, and only after the basic security check has been completed should any more detailed aspects of highly sensitive applications be examined. If it is necessary to verify the statements made during the interviews, then it would make sense to examine random samples of the relevant rules and concepts; or in the case of the infrastructure, by viewing the objects under examination on-site together with the contact person and by checking client and/or server settings in selected IT systems.

At the end of every safeguard, the person being interviewed should be informed of the results (i.e. if the safeguard implementation status = Unnecessary/Yes/Partially/No), and should be explained why the corresponding decision was made.

Action Points for 4.5.2 Performing the target/actual state comparison
▪ Prepare checklists in advance for each specialised area
▪ Explain the goals of the basic security check to the person being interviewed
▪ Ask the person what the implementation status is of each safeguard

- Verify the answers based on random samples of the object
- Inform the person being interviewed of the results

4.5.3 Documenting the results

The results of the basic security check should be documented so that they can be understood by all those involved and can be used as the basis for planning the implementation of those safeguards in which deficiencies still exist. BSI provides two additional tools to simplify documenting the results of the basic security check.

The first tool is the GSTOOL developed by the BSI. This software supports the complete IT-Grundschutz process, from recording the master data, defining protective requirements, performing the supplementary security and risk analysis, comparing the target/actual states (basic security check), to implementing safeguards. This provides convenient options for evaluating and auditing the results, for example by searching for certain entries, generating reports, analysing costs, and performing statistics functions.

There are also forms available as additional aids for IT-Grundschutz. There is a file in Word format for every module in the IT-Grundschutz Catalogues which can be used to record the results of the target/actual state comparison in a table for every safeguard in the module.

First, the following should be entered in the corresponding fields in the GSTOOL or in the forms:

- The name and number of the component or group of components this module was assigned to during modelling
- The location of the assigned component or group of components
- The date on which the information was entered and the name of the author
- The contact person interviewed

The actual results of the target/actual state comparison are entered in the table prepared for this purpose in the form. When entering the results, the fields should be completed as follows for each safeguard in the corresponding module:

- Degree of implementation (Unnecessary/Yes/Partially/No)
  In this field, the implementation status determined from the interview is entered for the corresponding safeguard.
- Implement by
  This field is generally not filled in during the basic security check. It serves as a placeholder for use when planning the implementation to document the deadline for the full implementation of the safeguard.
- Person responsible
  If it is clear when performing the target/actual state comparison which employee will be responsible for fully implementing a deficient safeguard, then the name of this person can be entered in this field. If it is unclear who is responsible, then the field should be left blank. The person responsible will then be specified later while planning the implementation, and the name of this person can be entered here at that time.
- Notes / reason(s) for non-implementation
  For safeguards whose implementation appears to be unnecessary, the reasons why the safeguards are unnecessary or the alternative safeguards implemented should be specified here. For safeguards that have not been implemented yet or only implemented in part, this field should document which recommendations of the safeguard still have to be implemented. Any other comments which could help to eliminate any shortcomings or which need to be taken into account in conjunction with the safeguard should also be entered here.

- Cost estimate
  For safeguards that have not been implemented yet or only implemented in part, an estimate of the financial and personnel resources needed to eliminate the shortcomings can be entered in this field.

Action Points for 4.5.3 Documenting the results
▪ Enter the master information for each target object in the tool, database, or form
▪ Enter information on the basic security check and the implementation status
▪ Make a note of the fields and placeholders intended for use when planning the implementation

4.6 Supplementary security analysis

The standard IT-Grundschutz safeguards are generally appropriate and adequate for typical business processes, applications, and IT systems with normal protection requirements. In certain cases, the special security safeguards determined in a risk analysis will be needed to supplement the IT-Grundschutz safeguards.

4.6.1 Two-stage approach of the IT-Grundschutz Methodology

For efficiency reasons, the IT-Grundschutz methodology uses a two-stage approach. In the first stage, the protection requirements of the object in the information domain are determined. With the help of the model created, typical threats and the corresponding standard security safeguards are assigned to the target objects. When deciding which threats and safeguards to assign, assume a typical application scenario and normal protection requirements. Based on the modules in the IT-Grundschutz Catalogues, this procedure can be used to quickly and efficiently increase the level of security in the information domain. In summary, the first stage serves to point out the security safeguards that eliminate the basic risks almost always present in a real information domain. The basic risks are therefore thoroughly handled already after the first stage of the IT-Grundschutz Methodology.

Furthermore, the second stage examines which other risks are relevant to the information domain and need to be taken into account.

4.6.2 Procedure for the supplementary security analysis

The supplementary security analysis is to be performed on all target objects in the information domain to which one or more of the following applies:

- The target objects have high or very high protection requirements in at least one of the three basic values – confidentiality, integrity, or availability
- The target objects could not be adequately depicted (modelled) with the existing modules in the IT-Grundschutz Catalogues
- The target objects are used in operating scenarios (e.g. in environments or with applications) that were not foreseen in the scope of IT-Grundschutz

The goal in this case is to decide for every single target object if additional risk analyses are required. Examples of applications or IT systems for which a supplementary security analysis is recommended include the online banking services provided by a financial service provider and IT systems with special, real-time operating systems.

To reduce the amount of work required, the target objects should be placed in suitable groups before performing supplementary security analysis. This applies, for example, to critical communication links as well. Such links can often be divided into groups such as “critical network sections”, “subnetworks”, “communication lines”, etc.

Valid reasons for or against an additional risk analysis must be stated clearly in a **management report** for every target object or group of target objects having one or more of the above characteristics. The target objects requiring an additional risk analysis are consolidated into risk areas. This should help point out which areas require an additional risk analysis.

The basis for the decisions made in the context of the supplementary security analysis includes the business objectives of the organisation, their basic risk principles, and possibly the resource priorities as well. The management report is to be submitted to management for approval. Management is therefore responsible for the report.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 10

Based on the protection requirements determined and the special operating conditions, a series of supplementary security analyses need to be performed in the BOV. The following table shows an excerpt from the results of these analyses:

Target object	Supplementary security analysis, excerpts from the management report
Domain controller S2	Due to its primary administrative function, high requirements are placed on the Domain Controller S2 in terms of the integrity. The system is already equipped with some internal mechanisms to protect against deliberate or unintentional manipulation. Some additional technical safeguards were checked but were then rejected due to incompatibility with the other products used. The IT management therefore suggests fulfilling the higher security requirements place on system S2 at the organisational level by having the IT audit section perform regular and frequent audits. In this case, a more detailed risk analysis is not required for S2.
Critical N1-N2/Internet communication links	The number of threat scenarios resulting from connecting the BOV to the Internet increased constantly during the reporting period. The problems with spam and malware increase particularly dramatically. IT management therefore recommends performing a risk analysis for the Internet connection.
Critical N3-S3/S4/S5/N2 communication links	The communication links listed have higher requirements in terms of availability. When reorganising the technical network layout, which is planned for next quarter and for which approval has already been obtained, central switch N3 will be eliminated. The new layout will be designed redundantly to thoroughly avoid single points of failure. Since the critical communication links stated are only temporary solutions anyway, IT management initially decided not to perform a risk analysis for these connections.
Server room R E.03 in Berlin	The availability requirements for the information technology operated in room R E.03 in Berlin are substantial. The results of a previous risk analysis for this server room are available, but the results are outdated. IT management therefore recommends performing a new risk analysis for room R E.03 in Berlin.

The complete management report is submitted to management for approval.

Note: The suggestions from the IT management at the BOV listed in the table above are examples and not the actual recommendations of the BSI for this fictitious application case.

4.6.3 Risk Analysis based on IT-Grundschutz

The job of a risk analysis in the context of information security is to identify any relevant threats to the information domain and estimate the possible risks resulting from these threats. The goal is to reduce the level of risk to an acceptable level by implementing the appropriate safeguards, to make the residual risks apparent, and in this manner to systematically control the overall (total) risk.

In the context of the IT-Grundschutz Methodology, management decides which target objects should be subjected to a supplementary security analysis based on the management report. The work required to perform the risk analyses is therefore concentrated on those areas in which the organisation believes such risk analyses will be useful and beneficial to the organisation.

To implement the decisions made in the course of the supplementary security analysis, BSI recommends performing a *risk analysis based on IT-Grundschutz* as described in BSI Standard 100-3.

The methodology described there can be integrated into the IT-Grundschutz process as follows:

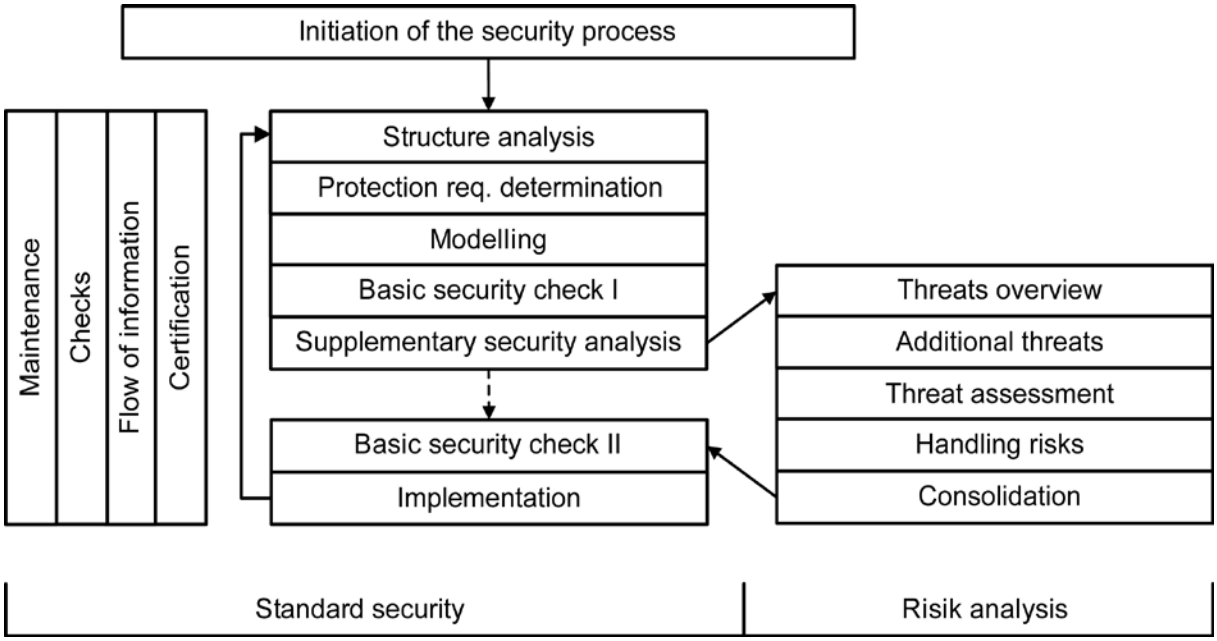


Figure 10: Integrating the risk analysis into the IT-Grundschutz process

The focus is on the following question: Which threats to the information domain are not adequately handled or not even considered at all in the standard IT-Grundschutz security safeguards?

In order to answer this question, the following additional steps in the overview below are recommended by the *risk analysis based on IT-Grundschutz*:

- Preparing the overview of threats
  In this initial step, a list of the relevant IT-Grundschutz threats is created for every target object to be analysed.
- Determining additional threats
  Additional threats resulting from the specific operating scenario are then added in this step to the threats taken from the IT-Grundschutz Catalogues. This is done in a brainstorming session.
- Threat assessment
  Check for every target object and every threat if the security safeguards already planned or implemented provide sufficient protection. The criteria for this check are the completeness, strength, and reliability of the protection mechanism.
- Selecting safeguards for handling risks
  The management level must specify how the identified risks should be handled. Generally, suggestions and options will be worked out by IS Management. The following options are available for handling risks:
  - Risks can be reduced through appropriate security safeguards
  - Risks can be avoided (e.g. by restructuring business processes or the information domain)
  - Risks can be transferred (e.g. by outsourcing or through insurance policies)

- Risks can be accepted

The decisions on how to handle the various security risks must be documented in the security concept. When documenting the decisions, the residual risk must be assessed and documented so the reasoning can be understood by all.

- Consolidating the security concept
  Before you can continue with the original IT-Grundschutz process, the supplementary security concept must be consolidated. During consolidation, the suitability, interactions, user friendliness, and appropriateness of the security safeguards are all checked.

In addition, how to apply the methodology when the information domain includes target objects for which IT-Grundschutz does not yet contain a suitable module is explained in the *risk analysis based on IT-Grundschutz.*

A detailed description of the methodology can be found in BSI Standard 100-3.

Important: The *risk analysis based on IT-Grundschutz* is a method for determining the security precautions that go beyond the security safeguards stated in the IT-Grundschutz Catalogues, if this is necessary. Although this methodology has been simplified in comparison with many other similar procedures, it is often accompanied by a considerable amount of work. In order to eliminate the most important security problems as quickly as possible, it is sometimes appropriate to implement the IT-Grundschutz safeguards completely *first* and only perform a risk analysis *after that* (in contrast to the scheme stated above). Although this means repeating some of the steps, the IT-Grundschutz safeguards will be implemented more quickly. This alternative order is particularly appropriate when both of the following statements apply:

1. The information domain under examination has already been implemented and is in use
2. The present target objects can be adequately modelled with the existing IT-Grundschutz modules

For information domains in planning or those with untypical technologies or operating scenarios, the original order described above is recommended. The following table summarises the advantages and disadvantages of the two alternative orders:

Risk analysis immediately after the basic security check	**Risk analysis after completely implementing the IT-Grundschutz safeguards**
Potential advantages: ▪ It avoids additional expense since no safeguards are implemented that may have to be replaced by stronger safeguards after the risk analysis. ▪ Any high-security safeguards required are identified and implemented earlier.	Potential advantages: ▪ IT-Grundschutz safeguards are implemented earlier since the risk analysis is often complicated. ▪ The basic security gaps in are dealt with first before the advanced threats are analysed.
Potential disadvantages: ▪ IT-Grundschutz safeguards are implemented later since the risk analysis is often complicated. ▪ Basic gaps in security may be neglected while analysing the advanced threats.	Potential disadvantages: ▪ It may result in additional expense since some of the IT-Grundschutz safeguards implemented will need to be replaced by stronger safeguards after the risk analysis. ▪ Any high-security safeguards required are identified and implemented later.

It is also important to know that a *risk analysis based on IT-Grundschutz* is frequently easier to perform when it is applied to one small aspect of the information domain after another. For example, as a first step, the analysis may be restricted to the physical building infrastructure, i.e. to protection

against fire, water, and unauthorised access as well as to ensure proper power supplies and air conditioning is available.

In many government agencies and companies, procedures for risk analysis and for handling risks have already been implemented. To achieve uniform application of the methodology, it may be appropriate in such cases to expand the existing method to information security and, if necessary, apply only some aspects of BSI Standard 100-3. Internationally, a series of different approaches have been established for performing risk analyses in the area of information security. These methods differ in terms of the degree of detail, the level of formality, and which areas they focus on. Depending on the corresponding conditions in an organisation and the type of information domain, it may be appropriate to use an established method or another, modified method to analyse the information risks as an alternative to BSI Standard 100-3.

The basic procedure used in an organisation for performing risk analyses should be documented in a guideline, which should then be approved by management. The **guideline for performing risk analyses** should contain the following aspects, among others:

- What prerequisites must be fulfilled in the context of the supplementary security analysis to decide not to perform a risk analysis?
- Under what conditions is a risk analysis absolutely necessary?
- Which method and/or which standard will be used as the basis for risk analyses?
- How will the selected method be adapted to the special interests of the organisation?
- Which organisational units are responsible for which subtasks in the risk analysis?
- How will the risk analyses be integrated into the security process, for example before or after implementing the IT-Grundschutz safeguards?
- Which reports must be submitted in the context of risk analyses?

Action Points for 4.6 Supplementary security analysis
▪ Document the basic procedure used in an organisation for performing risk analyses in a guideline and submit the guideline to management for approval.
▪ Determine for which target objects or groups of target objects a risk analysis should be performed
▪ Write the management report for the supplementary security analysis
▪ Submitted the management report to management for approval
▪ If necessary, systematically work through BSI Standard 100-3 “Risk analysis based on IT-Grundschutz”
▪ Integrate the results of the risk analyses into the security concept

5 Implementing the security concept

This chapter presents various aspects that must be considered when planning and implementing security safeguards. It describes how to plan, execute, supervised, and monitor the implementation of security safeguards.

When creating the security concept, the structure analysis, protection requirements determination, and modelling are performed for the information domain being examined. In addition, the results of the basic security check, and in particular of the subsequent target/actual state comparison are also available by this time. If a risk analysis has been performed for selected areas, then the suggestions for additional safeguards worked out should also be available and taken into account thereafter.

There are usually limited financial and personnel resources available for implementing the safeguards. The goal in the following steps is therefore to achieve the most efficient implementation possible of the intended security safeguards. An example of the procedure is found at the end of this chapter.

5.1 Viewing the results of the examination

First, the missing or only partially implemented IT-Grundschutz safeguards should be evaluated in an overall view. All unimplemented or only partially implemented safeguards can then be extracted from the results of the basic security check and summarised in a table.

Risk analyses can then be used to identify any additional safeguards which need to be implemented. These should also be documented in the form of a table. These additional safeguards should be assigned to the target objects examined during modelling and the corresponding IT-Grundschutz modules according to their subject area.

5.2 Consolidating the safeguards

In this step, you first consolidate the security safeguards which still need to be implemented. If additional risk analyses were performed, then additional security safeguards may have been identified that supplement or even replace the safeguards from the IT-Grundschutz Catalogues. In this case, it should be examined which IT-Grundschutz safeguards do not have to be implemented since they will be replaced by higher quality security safeguards.

Since recommendations are made in IT-Grundschutz for a variety of different types of organisations and technical configurations, the safeguards selected may need to be specified in more detail and adapted to reflect the organisational and technical circumstances present in the corresponding organisation. Furthermore, all security safeguards should be reviewed one more time to check if they are suitable: they must provide effective protection against the potential threats and be able to be implemented in practice, which means they may not, for example, hinder organisational processes or weaken other security safeguards. In such cases, it may be necessary to replace certain IT-Grundschutz safeguards with adequate, alternative security safeguards.

To be able to understand how the actual list of safeguards was created and refined later on, this process should be suitably documented.

Further information on consolidating the security safeguards can also be found in BSI Standard 100-3.

Examples:

- In a risk analysis, it was determined that, in addition to the IT-Grundschutz safeguards, smart card-supported authentication and local encryption of hard disks was needed on the clients used for processing personnel data. These additional safeguards would replace safeguard S 4.48 *Password Protection under NT-based Windows systems* for the clients used to process personnel data.

- In the basic security check, it was determined that safeguard S 1.24 *Avoidance of Water Pipes* has not been implemented, and due to structural considerations, it would not be cost-effective to implement this safeguard. Instead, metal sheeting to channel any leaking water are to be installed under the water pipes, which will also be monitored by a water alarm device. The alarm will send a signal to the caretaker so that when a water pipe leaks, the leaked water can be detected and contained quickly.

5.3 Estimation of the costs and personnel required

Since the budget for implementing security safeguards is practically always limited, it is necessary to determine the cost of investment and the amount of personnel required to implement each safeguard specified for implementation. A distinction should be made here between one-time and recurring investment/personnel costs. Experience has often shown that at this point, savings in technology often result in high recurrent personnel costs.

In this context, it is necessary to determine if all safeguards identified can be implemented economically. If there are any safeguards which cannot be financed, then consideration should be given as to which alternative safeguards could be used as replacements and if the residual risk resulting from the failure to implement a given safeguard is acceptable. This decision must be documented as well.

If the estimates of the required financial and personnel resources are available, then you can skip to the next step. In many cases, though, a decision must be made as to how many resources should be used to implement the security safeguards. It is recommended to prepare a presentation of the results of the security analysis for the person(s) responsible for making the decision (management, IT Manager, IT Security Officer, etc.). To increase awareness of security, the security vulnerabilities identified (missing or only partially implemented security safeguards) should be presented in the order of their protection requirements. In addition, it is also appropriate to summarise the costs and resources expected to implement the missing safeguards. A decision regarding the budget should then be made following this presentation.

If the budget required to adequately implement all the missing safeguards cannot be provided, then the residual risk resulting from not implementing or delaying the implementation of certain safeguards should be pointed out. The “cross-reference” tables from the IT-Grundschutz resources can be used to determine the residual risk. The cross-reference tables provide an overview for every module of which safeguards protect against which threats. Similarly, this table can also be used to determine which threats in the IT-Grundschutz Catalogues are not covered adequately. The residual risk resulting from any threats introduced accidentally or deliberately should be described clearly and presented to management for a decision. The remaining steps can only be performed after management has decided that the residual risk is acceptable since management bears the responsibility for the consequences.

5.4 Determining the order of implementation of the safeguards

If the existing budget or personnel resources are not adequate to permit all missing safeguards to be implemented immediately, then the order in which these safeguards will be implemented must be specified. When determining the order, the following aspects should be taken into account:

- The order of implementation should be based initially on the lifecycle classification of the safeguards. Every module contains an overview of which safeguards should be implemented in which lifecycle phase, i.e. the chronological order in which they should be implemented. You should, of course, start with the safeguards in the "Planning and design" phase before working on the safeguards in the "Implementation" and "Operation" phases.
- In addition, every safeguard is classified according to how necessary it is to obtain IT-Grundschutz Qualification. The qualification level (A-Entry, B-Secondary, C-Certificate, Z-Additional, and K-Knowledge) of a safeguard usually provides information on its significance in

the security concept. In most cases, the A-level safeguards are especially important and their implementation should be given the highest priority.

- For some safeguards, the chronological order is determined automatically by the logical relationships. For example, safeguards S 2.25 *Documenting the system configuration* and S 2.26 *Designation of an administrator and a deputy* are both very important, but it is hardly possible to implement S 2.25 without an administrator.
- Some safeguards have a wide-ranging effect, but other safeguards have only a limited, local effect. It is often appropriate to look at the range of the effect.
- Some modules have a larger impact on the desired security level than others. Safeguards from such modules should be given higher priority, especially if they eliminate vulnerabilities in areas requiring a high level of protection. For example, servers should be secured first (e.g. by implementing module 3.101 *General servers*) and then the clients connected to them should be secured.
- Modules that have a conspicuously large number of missing safeguards represent areas with a large number of vulnerabilities. They should also be given higher priority.

The decision on which security safeguards to implement or delay and where residual risks will be accepted should be documented carefully for legal reasons. When in doubt, additional opinions should be sought out and documented as well in order to provide evidence that the required level of care was taken in case of disputes later.

5.5 Specifying the tasks and responsibility

After determining the order of implementation of the safeguards, it must be specified who will implement which safeguards and by when they must be implemented. Experience has shown that without such a specification, implementation of the safeguards can be delayed substantially, or they may not be implemented at all. It must be ensured when specifying the person assigned to be responsible possesses the skills and authorities necessary to implement the safeguards and that this person is provided with the required resources.

The person responsible for monitoring implementation and to whom to report after completing the implementation of each safeguard should also be specified. The IT Security Officer is usually specified as the person to be notified upon completion. Regular checks of the progress of implementation should be performed so that the implementation tasks are not delayed.

The implementation plan, which is finished now, should contain at least the following information:

- Description of the target object and its operational environment
- Number of the module under consideration
- Names and descriptions of the safeguards
- Implementation schedule
- Size of the budget
- Person responsible for implementation
- Person responsible for monitoring implementation

5.6 Safeguards accompanying implementation

It is also extremely important to design and plan the implementation of any additional safeguards which will accompany the implementation of a given safeguard. Such safeguards include, in particular, awareness-raising safeguards intended to emphasise the need for information security and

informing the employees who will be affected by the new security safeguards of the necessity and consequences of the safeguards.

The affected employees must also receive training on how to implement and apply the new security safeguards correctly. When the corresponding employees have not received the required training, the safeguards are often not implemented and lose their effectiveness when the employees feel they were not adequately informed, which then results in a disapproving attitude towards information security.

Example: Bundesamt für Organisation und Verwaltung (Federal Agency for Organisation and Administration, BOV) - Part 11

The steps above will be described in excerpts based on the fictitious BOV. The following table shows some of the safeguards to be implemented and their estimated costs.

Target object	Module	Safeguard	Status	Costs	Notes
Entire organisation	1.9	S 2.11 Provisions governing the use of passwords	P	a) €0 b) 2 MD c) €0/year d) 0.5 MD/year	
Server room R 3.10	2.4	Z 1 Installation of flashing to drain off water with monitoring via a water alarm device which alerts the caretaker.	N	a) €4000 b) 3 MD c) €0/year d) 1 MD/year	Replaces safeguard S 1.24
Server S4	3.101	S 1.28 Local uninterruptible power supply	N	a) €1000 b) 1 MD c) €0/year d) 0.5 MD/year	
C1 group of clients	3.207	Z2 Smart card-based authentication plus local encryption of the hard disks	N	a) €1400 b) 2 MD c) €0/year d) 2 MD/year	This additional safeguard replaces safeguard S 4.1 in module 1.9
...					

Key:

- Safeguard
  Z1 = additional safeguard 1 (in addition to the IT-Grundschutz safeguards)
- Status (= implementation status)
  P = Partially implemented, N = Not implemented
- Costs:
  a) = one-time investment costs
  b) = one-off personnel expenses (MD = man-days)
  c) = recurring investment costs
  d) = recurring personnel expenses (MD = man-days)

The table below shows an excerpt of the implementation plan that would result from the management decisions entered in the table above.

Implementation plan (as of 01.09.20xy)

Target object	Module	Safeguard	To be implemented by	Responsible	Size of budget	Notes
Entire organisation	1.9	S 2.11 Provisions governing the use of passwords	31.12. 20xy	a) Mr. Miller b) Mrs. Meier	a) €0 b) 2 MD c) €0/year d) 0.5 MD/year	
Server room R 3.10	2.4	Z 1 Installation of flashing to drain off water with monitoring via a water alarm device which alerts the caretaker.	30.04. 20xy	a) Mr. Schmitz b) Mr. Hofmann	a) €1000 b) 2 MD c) €0/year d) 1 MD/year	Installation of flashing only under the fresh water and sewage pipes
Server S4	3.101	S 1.28 Local uninterruptible power supply	31.10. 20xy	a) Mr. Schulz b) Mrs. Meier	a) €500 b) 1 MD c) €0/year d) 0.5 MD/year	
C1 group of clients	3.207	Z2 Smart card-based authentication plus local encryption of the hard disks	31.12. 20xy	a) Mr. Schulz b) Mrs. Meier	a) €1400 b) 2 MD c) €0/year d) 2 MD/year	
...						

Key:

- Responsible:
  a) = Responsible for implementation of the safeguard
- b) = Responsible for monitoring its implementation
- Size of budget: The following are available for implementing the safeguard
  a) = one-time investment costs
- b) = one-time personnel expenses (MD = man-days)
- c) = recurring investment costs
- b) = recurring personnel expenses (MD = man-days)

The implementation of the safeguards can be monitored and controlled based on this information.

Action Points for 5 Implementing the security concept

- Summarise missing or partially implemented IT-Grundschutz safeguards as well as any additional security safeguards in a table
- Consolidate the security safeguards, i.e. eliminate any unnecessary safeguards, adapt general safeguards to the corresponding situation and check the suitability of all safeguards.
- Determine the one-time and recurring costs and expenses required to implement the safeguards.
- Determine the replacement safeguards for those safeguards that cannot be financed or implemented.

- Decide which resources should be used to implement the safeguards.
- If necessary, point out the residual risk and obtain a decision relating to the residual risk from management.
- Specify, provide reasons for, and document the order of implementation of the safeguards.
- Specify the deadlines for implementation and assign the persons to be responsible for the safeguards.
- Monitor the implementation and the ability to maintain the deadlines.
- Train and raise the awareness of the affected employees.

6 Maintenance and continuous improvement of the information security

In order to be able to maintain and continuously improve the information security process, you must not only implement adequate security safeguards and continually update documents, but also review the effectiveness and efficiency of the IS process itself on a regular basis. A performance review and evaluation of the IS process should be performed regularly by management (management appraisal). If necessary (for example when security incidents occur with increasing frequency or there are serious changes to the given conditions), meetings must also be held between the routine meeting dates. All results and decisions must be clearly documented so they can be understood later.

6.1 Checking the information security process at all levels

Checking the information security process is essential since, on one hand, the check will detect and help eliminate errors and vulnerabilities and, on the other hand, the efficiency of the IS process can be optimised. The goal of the check is to improve the practicality of the strategy, safeguards, and organisational procedures.

The essential aspects to consider during the check are presented in the following.

6.1.1 Methods for checking the information security process

To check and improve the efficiency of the information security process, procedures and mechanisms should be set up that check the implementation of the selected safeguards and that check the effectiveness and efficiency of the safeguards. The information security strategy should therefore contain key statements on measuring the achievement of the stated objectives. The basis for such measurements may include, for example:

- Detecting, documenting, and evaluating security incidents
- Implementing exercises and tests to simulate security incidents and documenting the results
- Performing internal and external audits and checking the data protection
- Certification according to the security criteria specified

The success of the safeguards implemented should be checked in the context of internal audits. It is important in this case that such audits are not performed by the persons involved in the development of the security concept. It may be appropriate in such cases to contract external experts to perform such checks and audits.

Since the cost of an audit depends on the complexity and size of the information domain, the requirements can also be implemented well even by small organisations. In small organisations, it may be sufficient just to check the technical aspects of IT systems on an annual basis, check the existing documentation to determine if it is up-to-date, and hold a workshop in which the problems and experiences with the security concept can be discussed may be sufficient in small organisations.

6.1.2 Checking the implementation of security safeguards

Based on the task list and the schedule, which must be available in the implementation plan, you can check the extent to which the tasks have been performed and the schedule is being maintained. An important prerequisite for maintaining the planned security safeguards is appropriate resource planning. It therefore makes sense to ensure that adequate financial and personnel resources have been made available during the check. Checking the information security process not only serves to check the activities as part of the security concept, but also to detect planning errors in time and to adapt the security strategy in case it proves to be unrealistic.

After implementing and introducing the new security safeguards, the IT Security Officer should check in particular if they are adequately accepted by the employees. If it is determined that the new safeguards have not been accepted, then they are sure to fail. The causes for this must be found and eliminated. This usually simply means explaining why they are important to those affected.

Security audit

The security safeguards contained in IT-Grundschutz can also be used to perform an audit of the information security. It is recommended to use the same procedure here as for the basic security check. It is helpful and more efficient to create a checklist for each module in the IT-Grundschutz Catalogues based on the safeguard descriptions that is then specially adapted to the organisation. This facilitates auditing and improves the reproducibility of the results.

ISO 27001 certification on the basis of IT-Grundschutz

Certification is another method used to check the level of implementation of the security safeguards and if the security objectives have been achieved. For certification, a qualified, independent agency professionally examines and evaluates the management and the information security implementation. Through certification according to ISO 27001 based on IT-Grundschutz, an organisation obtains understandable, repeatable, and comparable audit results. In addition, certification also documents the fact that the organisation has implemented both ISO 27001 as well as IT-Grundschutz with the required detail.

6.1.3 Suitability of the information security strategy

To enable successful control and management of the security process, management must be provided with an overview of the extent to which the security objectives can actually be achieved through the security strategy used.

Updating the security objectives, conditions, and security concept

From a long-term perspective, it is also necessary to check the security objectives specified and the general conditions. In rapidly changing industries in particular, it is very important to modify the security policy and security strategy accordingly.

Operational (e.g. the use of new IT systems or moving to a new location) and organisational changes (e.g. outsourcing) as well as changes to legal requirements must be incorporated into the security concept when planning these changes. The security concept and the corresponding documentation must be updated every time such a change is made. They must also be taken into account in the organisation's change process. To do this, the information security process must be integrated into the organisation's change management.

Examination of cost-effectiveness

Another issue that has to be constantly monitored is the cost-effectiveness of the security strategy and of specific security safeguards. The cost of information security is very difficult to determine, but it is often helpful when planning further developments to check if the costs actually incurred match the planned costs or if other alternative, less resource-intensive security safeguards could be implemented. It is also important to regularly state the benefits of the existing security safeguards.

Feedback from internal and external personnel

Feedback on errors and vulnerabilities in the processes generally not only come from the information security organisation or through audits, but also from employees, business partners, customers, or representatives. The organisation must therefore specify an effective method for handling complaints and other types of feedback from employees and outside sources. Complaints from customers and employees may also be an indication of dissatisfaction. Any dissatisfaction encountered should be counteracted as soon as it arises since the hazards arising from deliberate actions or negligence which could result in disruptions to operations are much lower when the employees are satisfied.

A clearly defined procedure and clearly specified authorities for handling complaints and reports of problems must be provided to the organisational entity responsible for this. This is necessary so that complaints can be responded to as quickly as possible, which provides the person providing the information with the feeling that they are being taken seriously. The problems reported must be evaluated, and the need for action must be estimated. The organisation must then implement appropriate correction safeguards to eliminate the causes of the errors and to prevent them from re-occurring.

6.1.4 Integrating the results into the information security process

The results of the success review are required to improve the IS process. The results may indicate that the security objectives, security strategy, or security concept need to be changed, or that the information security organisation must be adapted to the present requirements. In some circumstances, it may be appropriate to make fundamental changes to the IT environment or to the business processes, for example when security objectives cannot be achieved or can only be achieved with difficulty (i.e. at great financial or personnel expense) under the previous general conditions. If large-scale changes are made or comprehensive improvements are implemented, then the management cycle comes to an end and the planning phase must be started again.

The checks in each of the subject areas must be performed by suitable people who have the required skills and are independent. The people who created the concepts should not perform any completion or plausibility checks.

The basic procedure used in an organisation to check and improve the information security process should be documented in a corresponding policy, which should then be approved by management. The **policy for checking and improving the information security process** in particular should contain policies on how to perform internal information security audits and how to integrate the results into the change process. In general, test results and reports are to be considered highly confidential information and must be provided with special protection.

Action Points for 6.1 Checking the information security process at all levels
▪ Document the basic procedure used in the organisation for checking and improving the information security process in a corresponding policy and submit the policy to management for approval.
▪ Integrate measurements of the achievement of objectives into the security strategy
▪ Check to make sure the implementation plan is followed
▪ Check the implementation of the selected safeguards
▪ Check the effectiveness and efficiency of the selected safeguards
▪ Check if the security safeguards have been accepted, and improve if necessary
▪ Be aware of conflicts of interest between the roles of the author and the examiner
▪ Ensure that the results of the tests and checks are kept confidential
▪ Check the suitability and actuality of the security objectives, security strategies, and security concept
▪ Check the appropriateness of resources provided and the cost-effectiveness of the security strategy and security safeguards
▪ Integrate the results of the checks into the information security process in the form of improvements

6.2 The flow of information in the information security process

As a result of the checks and improvements to the information security process, a variety of reports, audit reports, security test results, reports of security-related events, and other information security documents are created in the organisation. The documents must be informative and understandable for the corresponding target group. Since not all this information is of interest to management, it is the job of the IT Security Officer and the IS Management team to collect, process, prepare, and present this information clearly yet briefly.

6.2.1 Reports to management

In order for the management to be able to make the right decisions on controlling and managing the information security process, they need basic information relating to the information security status. This data should be prepared in management reports that provide this data and cover the following points, among others:

- Results of audits and data protection checks
- Reports on security incidents
- Reports on previous successes and problems in the information security process

Management must be informed regularly in an appropriate form by the IS organisation of the results of the checks and the status of the IS process. This includes pointing out any problems, successes, and potential for improvement. Management must take note of the management reports and initiate any safeguards that may be necessary.

6.2.2 Documentation in the information security process

For many reasons, the documentation of the IS process on all levels is key to its success. The following can only be ensured when sufficient documentation is available:

- Decisions are understandable by all
- Processes can be repeated and standardised
- Vulnerabilities and errors can be detected and prevented in the future

Depending on the subject and purpose of a document, the following different types of documentation may exist:

- Technical documentation and documentation of workflows (target group: experts)

  The current status of business processes and the IT systems and applications used by and for these business processes are described here. The level of detail of technical documentation is often a subject of controversy. One practical approach to take is to ensure that other people with comparable expertise can understand the documentation and that the administrator can depend on his knowledge, but must not depend on his memory, to restore the systems and applications. During security exercises and when handling security incidents, the quality of the documentation available should be evaluated and the results of the evaluation used to improve the documentation. This type of documentation includes, among other types:

  - Installation and configuration manuals
  - Instructions for re-starting after a security incident
  - Documentation of testing and release procedures
  - Instructions on how to respond to malfunctions and security incidents

- Instructions for employees (target group: employees)

  Security safeguards must be documented in the form of policies which can be understood by the employees. In addition, the employees must be informed of the existence and importance of these

policies, and must have received the corresponding training. This group of documentation consists of, for example:

- Workflows and organisational specifications
- Policies for Internet usage
- Responses to security incidents

- Documentation of management decisions (target group: management)

  Basic decisions on the information security process and security strategy must be recorded so that they can be understood and repeated at any time.

- Laws and regulations (target group: management)

  A number of different laws, regulations, and instructions may apply to the processing of information. The special requirements placed on business processes, IT operations, or information security as well as their consequences resulting from laws, regulations, and instructions in the case at hand should be documented.

It must be ensured that all documentation is kept up-to-date. The documentation must be integrated into the change process for this purpose.

6.2.3 Information flow and reporting routes

Prompt updating of the reporting routes and the specification of the flow of information are of key importance to maintaining the information security process. In addition, the results of the checks, tests, and audits performed also provide a useful basis for improving the information flow.

The basic specifications relating to the flow of information and the reporting routes should be documented in a corresponding policy, which should then be approved by management. The **policy on the flow of information and reporting routes** should regulate in particular the information flows critical to the information security process. The policy must differentiate between receiving and distributing information flows.

Using synergy effects for the information flow

Many organisations have already defined processes to provide services or IT support. Synergy effects can often be used, and aspects of information security can often be integrated into existing processes. For example, the reporting routes for IT security incidents can be integrated into IT support, or capacity planning can be expanded to include aspects of contingency planning.

Much of the information collected for security reasons can also be used for other purposes. In addition, security safeguards also have other positive side-effects, and the optimisation of the processes in particular pays off. For example, the appointment of information owners or the classification of information according to uniform evaluation criteria is often relevant for many areas of an organisation. An overview of the dependency of business process on IT systems and applications is not only useful for security management. For example, an overview it enables you to precisely associate IT costs which are often considered to be overhead to specific business processes or products.

Action Points for 6.2 The flow of information in the information security process
▪ The basic specifications for the flow of information and the reporting routes which are related to the information security process should be documented in a corresponding policy and submitted to management for approval.
▪ Inform management of the results of the checks and the status of the information security process
▪ If necessary, obtain the decisions for the required corrective safeguards
▪ Document all sub-aspects of the entire information security process understandably and keep the

documentation up-to-date

- If necessary, evaluate the quality of the documentation and improve or update it wherever necessary
- Keep the reporting routes relating to the information security process up-to-date
- Find synergies between the information security process and other management processes

7 ISO 27001 certification on the basis of IT-Grundschutz

In order to make the successful implementation of IT-Grundschutz clear to the outside world, the BSI has developed a certification scheme for information security. This scheme takes the requirements on management systems for information security found in ISO/IEC 27001 into account. The ISO 27001 certificate based on IT-Grundschutz or verification by an auditor provides companies and government agencies with the ability to make its information security efforts transparent to others. This can serve as a quality characteristic for customers and business partners both, and therefore provide the organisation with a competitive advantage.

There are many reasons why you should obtain ISO 27001 certification on the basis of IT-Grundschutz:

- Service providers use this trusted certificate to verifiably demonstrate that they have implemented the safeguards in accordance with IT-Grundschutz.
- Partner companies want to be informed of the level of information security their business partners are able to guarantee.
- Organisations that have recently been connected to a network are asked to provide evidence that the level of information security in their organisations is sufficient to rule out the possibility of any unacceptable risks arising due to the organisation's connection to the network.
- Organisations want to make it clear to their customers and the public how much effort they have put into achieving an adequate level of information security.

Since the IT-Grundschutz Methodology for security management described in this document and the recommended standard security safeguards in the IT-Grundschutz Catalogues have now become a virtual standard for information security, they could be used as a generally recognised set of criteria for information security.

The basis for awarding an ISO 27001 certificate on the basis of IT-Grundschutz is the audit performed by an external auditor who is certified with the BSI. The result of the audit is an audit report that is then presented to the certification department, which decides if the ISO-27001 certificate based on IT-Grundschutz should be awarded. Sets of criteria for the procedure are, in addition to the ISO 27001 standard, the IT-Grundschutz methodology described in this document and the IT-Grundschutz Catalogues of the BSI.

An ISO 27001 certificate based on IT-Grundschutz initially verifies that IT-Grundschutz has been successfully implemented in the information domain being examined. In addition, though, this certificate also demonstrates the following about the organisation:

- The organisation recognises the importance of information security
- The organisation has a functioning IS Management
- The organisation has achieved a defined level of security at a specific time

Further information on ISO 27001 certification and on certification as an ISO 27001 auditor on the basis of IT-Grundschutz can be found on the BSI web site (refer to [ZERT]).

Action Points for 7 ISO 27001 certification on the basis of IT-Grundschutz
▪ Read the information from the BSI on the qualification scheme and on the scheme for ISO 27001 certification on the basis of IT-Grundschutz ▪ Check if the efforts to obtain information security can be made clear based on confirmation from an auditor or on an ISO 27001 certificate on the basis of IT-Grundschutz ▪ If necessary, check if the information security management and security status meet the corresponding requirements

- If necessary, initiate the qualification or certification process

Appendix

Explanations of the damage scenarios

In the following, the questions for the damage scenarios in section 4.3.1 are listed as examples. These questions should be used as an aid to determine the protection requirements, especially the protection requirements for the applications. The questions should be modified accordingly or new questions added based on the individual requirements.

"Violation of laws, regulations, or contracts" damage scenario

These types of violations can result from the loss of confidentiality as well as from a loss of integrity or availability. The severity of the resulting damage will often depend on the specific legal consequences that could result for the organisation.

Examples of relevant laws (in Germany) are:

> The Constitution, the Civil Code, the Criminal Code, the Federal Data Protection Act, and the data protection laws of the individual states, the Social Security Statutes, the Commercial Code, the Works Committee Act, the Works Constitution Act, the Copyright Act, the Patents Act, the Information and Communication Services Act (IuKDG), the Control and Transparency in Business Act (KonTraG).

Examples of relevant regulations are:

> Administrative regulations, ordinances, and service regulations.

Examples of contracts:

> Service contracts in the area of data processing, contracts for maintaining the confidentiality of business secrets.

Questions:

Loss of confidentiality

- Is confidentiality of the data required by law?
- Is the disclosure of information likely to result in criminal prosecution or compensation claims?
- Are contracts involved that include a requirement to maintain the confidentiality of certain information?

Loss of integrity

- Is data integrity required by law?
- To what extent will a loss of integrity violate laws or regulations?

Loss of availability

- Would failure of the application result in the violation of any regulations or possibly even laws?
- Is certain information required to be available at all times by law?
- Are there any deadlines which absolutely must be met when using the application?
- Are there any contractual conditions requiring certain deadlines to be met?

"Impairment of the right to informational self-determination" damage scenario

When implementing and operating IT systems and applications, there is a risk of violating the right to informational self-determination and even of abusing personal data.

Examples of impairments to the right to informational self-determination include:

- Unauthorised collection of personal data without legal cause or the consent of the individual
- Unauthorised acquisition of information during the processing or transmission of personal data
- Unauthorised disclosure of personal data to third parties
- Use of personal data for a purpose other than for the purpose for which it was authorised and collected
- Manipulation of personal data in IT systems or during the transmission of personal data

The following questions can be used to estimate the possible consequences and the extent of any damage:

Questions:

Loss of confidentiality

- What harm could come to an individual if his or her personal data is not kept confidential?
- Is any personal data processed for unauthorised purposes?
- Is it possible when processing personal data for a valid reason that information could be obtained, for example, on the person's health or economic situation?
- What damage could be caused by the misuse of the personal data stored?

Loss of integrity

- What harm could come to an individual if his or her personal data were to be corrupted by accident or deliberately manipulated?
- When would the loss of integrity of any personal data first be noticed?

Loss of availability

- If an application were to fail or personal data was lost or even falsified due to a problem during transmission, is it possible that the affected person could experience adverse effects to his social position or even personal or economic disadvantages?

"Physical injury" damage scenario

The malfunctioning of an IT system or an application can immediately result in injury, disability, or even death. The extent of the damage must be evaluated based on the direct personal damage.

Examples of such applications and IT systems are:

- Medical monitoring computers
- Medical diagnosis systems
- Flight control computers
- Traffic routing systems

Questions:

Loss of confidentiality

- Could a person be physically or psychologically injured through the disclosure of his or her personal data?

Loss of integrity

- Could manipulating the program flow or data endanger someone's physical or mental health?

Loss of availability

- Does the failure of an application or IT system directly threaten the personal health of anyone?

"Impaired ability to perform tasks" damage scenario

The loss of the availability of an application or the integrity of the data in particular can substantially affect the ability of an organisation to perform its tasks. In this case, the severity of the resulting damage depends on the duration of the impairment and the extent to which the services offered are limited.

Examples of this are:

- Missed deadlines due to delays in the execution of administrative procedures
- Late delivery due to delays in the processing of orders
- Faulty production due to incorrect control parameters
- Insufficient quality assurance due to the failure of a test system

Questions:

Loss of confidentiality

- Is there any data whose confidentiality is necessary to be able to perform the tasks at hand (e.g. criminal prosecution information, investigation findings)?

Loss of integrity

- Could changes to data limit the organisation's ability to perform its tasks to the extent that the organisation is unable to operate?
- Would significant damage result if the tasks are performed even though the data is corrupt? When would unauthorised changes to the data first be noticed?
- Could corrupt data in the application being examined lead to errors in other applications?
- What would be the consequences if data is incorrectly assumed to belong to someone who did not actually generate it?

Loss of availability

- Can the failure of an application so severely affect the ability of an organisation to perform its tasks that the wait times for those affected are no longer tolerable?
- Would any other applications be affected by the failure of this application?
- Is it important to the organisation to have guaranteed access to applications as well as programs and data at all times?

"Negative internal or external effects" damage scenario

Various types of negative internal and external effects can result from the loss of one of the three basic values of confidentiality, integrity, and availability. Examples of these effects include:

- Damage to the reputation of an organisation
- Loss of confidence in the organisation
- Loss of employee morale
- Adverse effect on commercial relationships with partner organisations

- Loss of confidence in the quality of the work done by an organisation
- Loss of competitive ability

The level of damage depends on the severity of the loss in confidence or how widespread the internal or external effect is.

The causes for such damage can be very diverse:

- The inability of an organisation's to operate due to an IT system failure
- Publications containing errors due to manipulated data
- Incorrect orders due to poor warehouse management programs
- A failure to comply with confidentiality agreements
- Assigning of blame to the wrong people
- Inability of a department to perform its tasks due to errors in other areas
- Transferral of data from criminal investigations to interested third parties
- Leaking of confidential information to the press

Questions:

Loss of confidentiality

- What would be the consequences to the organisation as a result of the unauthorised publication of sensitive data stored for the application?
- Can the loss of confidentiality of saved data lead to a weaker competitive position?
- Would the disclosure of confidential data raise doubts about the organisation’s ability to maintain official secrecy?
- Could the disclosure of data lead to political or social insecurity?
- Could employees lose their confidence in the organisation as a result of unauthorised publication of data?

Loss of integrity

- What damage could result from the processing, distribution, or transmission of incorrect or incomplete data?
- Would the data corruption become publicly known?
- Could the publication of corrupt data hurt the reputation of the organisation?
- Could the publication of corrupt data lead to political or social insecurity?
- Could corrupt data lead to reduced product quality, and therefore tarnish the reputation of the organisation?

Loss of availability

- Would the failure of the application restrict the information services provided to external parties?
- Do application failures prevent the organisation from achieving its business objectives?
- When would the failure of the application first be noticed by an external party?

"Financial consequences" damage scenario

Direct or indirect financial damage can arise from a loss of confidentiality in data requiring protection, changes to data, or application failures. Examples include:

- Unauthorised release of results from research and development

- Manipulation of financially-relevant data in an accounting system
- Failure of an IT-controlled production system, which then results in reduced sales
- Unauthorised access to marketing strategy papers or sales figures
- Failure of a booking system at a travel agency
- Failure of an e-commerce server
- Breakdown of a bank's payment transactions
- Theft or destruction of hardware

The total amount of damage is comprised of the direct or indirect costs incurred, for example through damage to property, damage claims from third parties, and additional costs (e.g. restoration).

Questions:

Loss of confidentiality

- Could the publication of confidential information lead to compensation claims?
- Is there data in the application that could provide a third party (e.g. a competitor) with a financial advantage if accessed by the third party?
- Is any research data of significant value stored using the application? What would happen if such data was copied and passed on without permission?
- Could any financial damage result from the premature publication of sensitive data?

Loss of integrity

- Could any data relevant to accounting be manipulated in such a way as to cause financial damage?
- Could the publication of incorrect information lead to compensation claims?
- Could corrupted order data result in financial damage (e.g. for just-in-time production)?
- Could corrupt data lead to the wrong business decisions being made?

Loss of availability

- Would failure of the application adversely affect production, inventory management, or sales?
- If the application fails, would there be financial losses due to delayed payments or lost interest?
- How much would it cost to repair or restore the IT system if it fails, develops a fault, is destroyed, or is stolen?
- Could the failure of the application result in an inability make payments or to contractual penalties?
- How many important customers would be affected by a failure of the application?