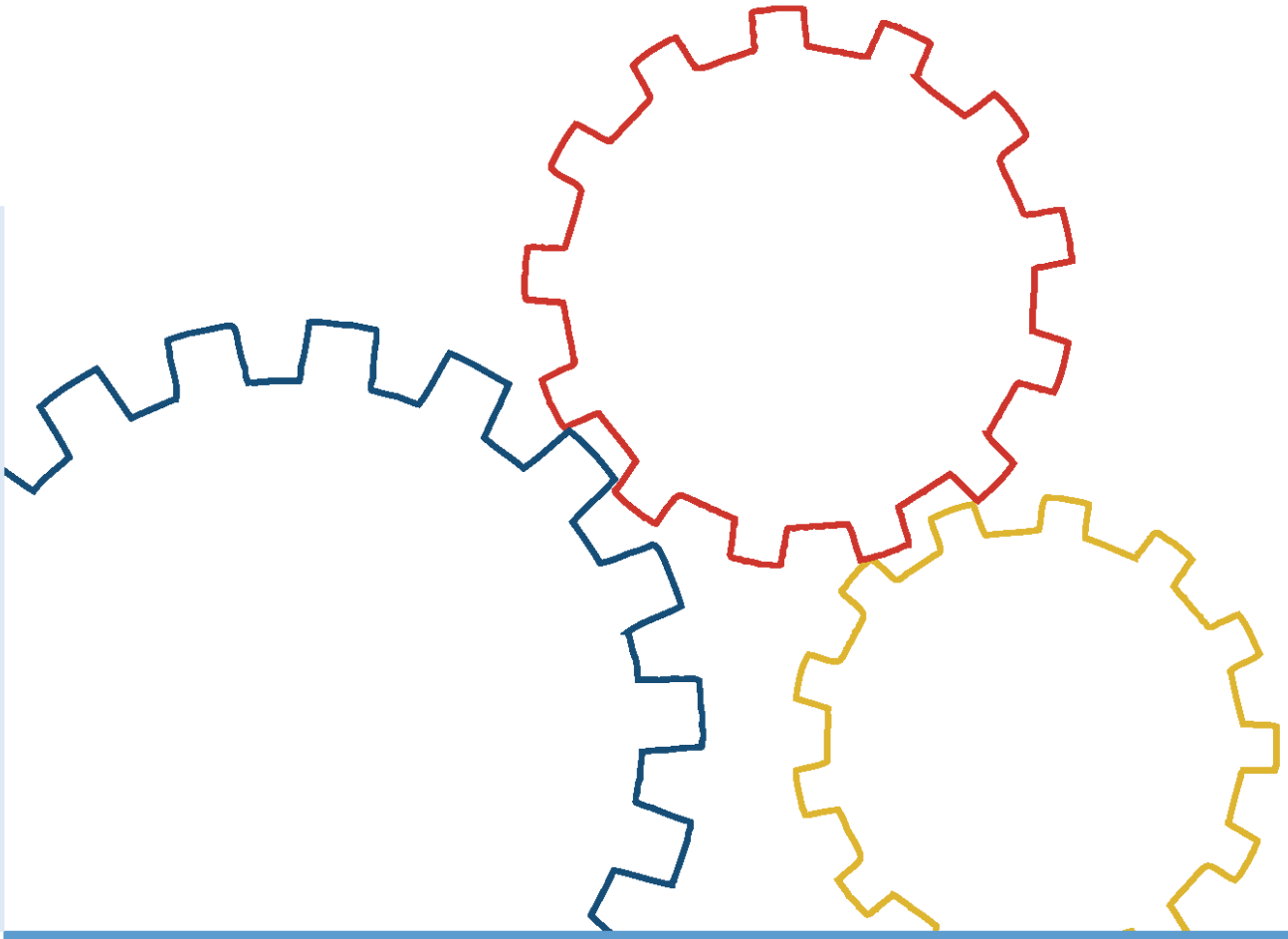
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 200-2

IT-Grundschutz Methodology



www.bsi.bund.de/grundschutz

Version 1.0

BSI-Standard 200-2

IT-Grundschutz Methodology

Version 1.0, October 2017

Table of contents

1 Introduction

1 Introduction

1.1 Version history

BSI-Standard 200-2 replaces BSI-Standard 100-2.

As per	Version	Changes
March 2017	CD 1.0	Redesigned based on BSI Standard 100-2 • Within the scope of modernisation of IT-Grundschutz, the methodologies for Basic Protection and Core Protection have been included in addition to the Standard Protection • Extension to include virtualisation, cloud, ICS and IoT safeguards • Clarification of roles and tasks of IT-SiBe and ISO • Adjustments to updating of ISO standards • More detailing of information classification • Information flow within information security process revised, adaptation to 100-4 • Exemplary BoV replaced by RecPlast
October 2017	Version 1.0	Inclusion of user comments • Mainly language-related clarifications • Change of German term “Aktiva” to “Assets”

1.2 Objective

With BSI-Standard 200-2 the BSI provides methodology for effective management of information security. This can be adapted to the requirements of organisations of various types and sizes. In BSI-Standard 200-2 this is implemented via the three methodologies “Standard Protection”, “Basic Protection” and “Core Protection”.

The methodology is based on the BSI-Standard 200-1 *Management systems for information security (ISMS)* (see [BSI1]) and thus also on ISO 27001 [27001]. This document shows how the basic framework for an information security management system presented in BSI-Standard 200-1 is specified by IT-Grundschutz. A management system for information security (ISMS) is the planned and organised course of action to achieve and maintain an appropriate level of information security.

IT-Grundschutz is an established standard for creation and maintenance of appropriate protection of any information of an organisation. The methodology continuously advanced by BSI offers both instructions for creation of an ISMS and a comprehensive base for risk analysis, verification of the present level of security and implementation of an appropriate degree of information security.

One of the most important objectives of IT-Grundschutz is to reduce the expenses of the information security process. For this, known approaches and methods for improvement of information security are combined and updated continuously. Additionally, in the IT-Grundschutz Compendium, BSI publishes methods with concrete security safeguards for typical business processes, applications, systems, communication links and rooms that can be implemented at the own organisation as needed. IT-Grundschutz considers all areas of an organisation, including production and manufacturing using Industrial Control Systems (ICS) as well as components from the field of Internet of Things (IoT).

By implementing organisational, personnel, infrastructural, and technical security safeguards, the “Standard Protection” approach makes it possible to attain a level of security for the considered business processes that is adequate for normal protection requirements and appropriate for protecting business-related information. Implementation of the “Basic Protection” approach attains a level of security that is significantly below the Standard Protection, but offers a good basis for ISMS beginners. The “Core Protection” approach can be used to preferably protect information and business processes requiring particular protection.

The IT-Grundschutz Methodology is extended regularly and adapted to current developments resulting from new processes, standards, and regulations, and above all resulting from the continuously advancing digitalisation. Due to the close exchange of experience with the users of IT-Grundschutz, new requirements and aspects are being included into the publication steadily. Thus, the users may use current ISMS recommendations for their organisation and may be able to quickly identify and remove typical security issues.

1.3 Addressees

The BSI-Standard 200-2 is primarily aimed at those who are responsible for security, experts, consultants and everyone who is familiar with the management of information security. It is also an appropriate foundation for those responsible for IT and ICS , managers and project managers who ensure that the aspects of information of their organisation or projects have been adequately taken into account.

IT-Grundschutz provides a cost-effective and targeted method for creating and implementing appropriate information security for organisations of any size and industry. The term "organisations" is used in the following text for companies, public agencies and other public and private organisations.

IT-Grundschutz can be used both by small and large organisations. However, it should be noted that all recommendations should be examined in the context of the particular organisation and should be adapted to the framework conditions.

IT-Grundschutz assumes that both the information and communication technologies as well as any present industrial control and automation technologies are administered by suitable qualified staff, i.e. that there is IT operation with clearly defined roles. This may reach from an individual administrator to one or more IT departments. The various activities within the security process are described on such basis.

1.4 Application

The BSI Standard 200-1 *Management Systems for Information Security (ISMS)* describes the general methods for the initiation and management of information security in an organisation. The present BSI-Standard 200-2 provides specific assistance on how to introduce a management system for information security step by step: Focus is on individual phases of such process as well as proven best-practice solutions.

The IT-Grundschutz Methodology provides a comprehensive framework for an ISMS and needs to be adapted to the individual environment of an organisation so as to set up a suitable management system for information security. A continuous and efficient process for information security requires performance of a number of actions. The IT-Grundschutz Methodology and the IT-Grundschutz Compendium provide information and practical implementation resources.

Furthermore, this standard provides the possibility of certification. This does not only enable an organisation to implement IT-Grundschutz, but also to prove quality of the own ISMS using an ISO 27001 certificate on the basis of IT-Grundschutz. The certificate also serves as a criterion for other organisations to inform themselves on the maturity level of an ISMS of another organisation.

Certification in accordance with ISO 27001 on the basis of IT-Grundschutz can also be used as a security requirement for possible cooperation partners to define the required level of the other organisation's information security.

Even if another methodology is used as a basis for ISMS, it still will be possible to benefit from IT-Grundschutz. IT-Grundschutz also offers solution approaches for individual tasks such as for creation of concepts or performance of auditing and certifications in the field of information security. Depending on the application area, individual modules, implementation recommendations or other auxiliary materials provided by IT-Grundschutz form a helpful basis for security management work.

1.5 Structure of BSI-Standard 200-2

Section 2 includes the most important steps for introducing an ISMS as well as for drawing up of a security concept.

Section 3 describes the possible design of the basic phase of initiating the information security process and the required background information to be able to make a well-founded decision on the approach suitable for the organisation for securing their information and business processes. A policy on information security is to be created as essential basis for further activities.

The security process requires setting up of suitable organisational structures and implementing a functional security management, see Section 4.

Various documentations must be created within the scope of a functional security process. Section 5 describes the things to be noted in this regard.

Section 6 will show the steps to be taken if Basic Protection is the chosen approach. The objective of Basic Protection, as a start on IT-Grundschutz, primarily is to achieve a broad and basic initial safeguard of all business processes and/or specialist methodologies of an organisation. After specification of the scope, selection and allocation of the IT-Grundschutz modules must be made and the sequence of their application is to be defined. An IT-Grundschutz Check is used to check the level of implementation of the basic requirements. Then, concrete actions for fulfilling the open requirements must be derived and implemented. Selection of one of the following approaches should maintain and improve the level of security achieved correspondingly.

Section 7 shows how to achieve preferred protection of the essential assets according to IT-Grundschutz using Core Protection. Here, the approach is highly based on the steps of the Standard Protection approach as described in the following.

Section 8 describes the Standard Protection approach. This first lists how the basic information on an information domain can be collected and simplified by forming groups. Subsequently, based on the business processes, the protection requirements for IT applications, systems, communication links and rooms must be determined. The appropriate modules and requirements from the recommendations in the IT-Grundschutz Compendium must then be selected for the relevant information domain – i.e. they are modelled in accordance with IT-Grundschutz. Security safeguards must be derived from the selected requirements. Before implementation of security safeguards, any present and additional security safeguards, determined e.g. by risk analysis on the basis of IT-Grundschutz in accordance with BSI-Standard 200-3 (see [BSI3]), must be integrated into the security concept.

Section 9 then describes how implementation of the identified and consolidated security safeguards is to be performed.

The core objective of an ISMS is to ensure the maintenance of information security and to continuously improve it. This issue is dealt with in Section 10.

The IT-Grundschutz approaches and the IT-Grundschutz Compendium are not only used for the security design, but also as a reference within the meaning of a security standard. By obtaining ISO 27001 certification based on IT-Grundschutz, an organisation can document internally and externally that it has implemented both ISO 27001 and IT-Grundschutz to the extent required. Section 11

provides a short overview on the steps required for this and on the conditions to achieve successful certification.

2 Information security management using IT-Grundschutz

Information constitutes an essential asset for companies and government agencies and so requires adequate protection. Today, the majority of information is generated, stored, transported, or processed further with the help of information technology (IT). State-of-the-art business processes in the fields of economy and administration without IT support are no longer imaginable today. With Industrial Control Systems (ICS) the information and communications technologies found their way into production and manufacturing as well as via Internet of Things (IoT) into almost any other area.

Inadequately protected information is a frequently underestimated risk factor that can threaten the existence of an organisation. At the same time, reasonable information protection and basic IT protection can be achieved with relatively modest resources.

2.1 Holistic concept

However, more than only purchasing anti-virus programmes, firewalls and data back-up systems is needed to achieve a demand-driven level of security for all business processes, information and also IT systems of an organisation. A holistic concept is important. This includes above all functional security management that is integrated into the organisation. Information security management (or briefly IS management) is the element of general risk management that aims to ensure the confidentiality, integrity and availability of information, business processes, applications and IT systems. This is a continuous process to monitor strategies and concepts on an ongoing basis for their performance and effectiveness and to update them as required.

Information security is not only a question of technology but rather depends substantially on the organisational and personnel environment. IT-Grundschutz accounts for this by describing both technical and non-technical security requirements for typical business areas, applications and systems using the state-of-the-art modules. In this context the focus is on practical and activity-based security requirements with the objective of keeping the barriers to entering the security process as low as possible and avoiding highly complex methodologies.

Using Basic Protection, Standard Protection and Core Protection, IT-Grundschutz offers various approaches to provide to the organisations, based on their type and size, corresponding instruments for protecting their information domains.

2.2 Management system for information security

BSI-Standard 200-2 describes how an efficient management system for information security can be set up and how the IT-Grundschutz Compendium can be used for this task. The IT-Grundschutz approaches combined with the IT-Grundschutz Compendium provide a systematic methodology to work out security concepts and practical security safeguards that have been successfully implemented by numerous public agencies and companies.

The modules in the IT-Grundschutz Compendium are subject to constant revision and current 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 public agencies and companies all documents on IT-Grundschutz are also available in English and in electronic form.

Business processes are increasingly linked together via information and communication technology. This is accompanied by increases in the complexity of the technical systems and with a high dependence on the correct operation of the technology. Therefore, the approach by all those involved must be planned and organised in order to implement and maintain an appropriate level of security. It is only possible to guarantee that this process is anchored in all business areas if it becomes a top management task. The highest level of management is responsible for the proper, targeted operation of an organisation, hence for guaranteeing information security internally and externally. They are thus responsible for initiating, controlling and monitoring the security process. This includes key strategic statements on information security, conceptual requirements and also the organisational

environment as well as sufficient resources for achieving information security within all business processes.

2.3 Responsibility for information security

In any case, responsibility for information security rests with the top management level; however, the task of “information security” usually is delegated to an information security officer. Up to now, the IT-Grundschutz documents used the term IT security officer as such term had been the most common term used by companies and public agencies. However, the term information security officer or briefly IS officer (ISO) is more accurate and correspondingly replaces the old denomination in IT-Grundschutz. Other versions include CISO (Chief Information Security Officer) or information security manager (ISM).

Information security comprises the comprehensive area of the protection of information, namely in and with IT, but also without IT or beyond IT. IT security is thus a subdivision of information security and deals specifically with the protection of the IT employed. In large organisations, there also can be a dedicated IT security officer in addition to the ISO. This person typically operates in the IT area, while the ISO reports directly to the management level.

If this framework does not exist in a given situation, as a first step an attempt should be made to implement the missing security safeguards at the "shop-floor" level. However, in each case, the objective is to raise awareness with the management for information security issues so that they bear the responsibility for it in the future. Although many aspects of the information security process can be initiated on the shop-floor and will result in a specific improvement in the security situation; there is no guarantee that such actions will lead to a permanent increase in the IT level of security.

2.4 Elements of IT-Grundschutz

Well-founded security management that works well is the essential foundation for the reliable and continuous implementation of security safeguards in an organisation. Therefore, in addition to detailed information in this document, there is an *Security management* module in the IT-Grundschutz Compendium. This is used both to achieve a homogeneous methodology for applying IT-Grundschutz and for including security management to an extent appropriate to its importance in certification in accordance with ISO 27001 on the basis of IT-Grundschutz.

In addition to the IT-Grundschutz approaches described in this standard, the IT-Grundschutz Compendium formulates state-of-the-art security requirements. In so doing, IT-Grundschutz follows a holistic approach. By suitably implementing organisational, personnel, infrastructural, and technical security safeguards, the “Standard Protection” makes it possible to attain a level of security that is adequate for normal protection requirements and appropriate for protecting business-related information. Implementation of the “Basic Protection” attains a level of security that is significantly below the Standard Protection, but offers a good basis for beginners. The “Core Protection” can be used to preferably protect information and business processes requiring particularly high protection. The modules of the IT-Grundschutz Compendium provide suitable “bundles” with security requirements for Basic Protection, Standard Protection and Core Protection applicable for typical processes, applications and components of information, communications and manufacturing technologies.

Based on the corresponding focus, these modules are divided into process-oriented and system-oriented modules and grouped together in a layer model based on matching topics. The process-oriented modules are included in the following layers:

- ISMS *(Information Security Management Systems)*
- ORP *(Organisation and Personnel)*
- CON *(Concepts)*
- OPS *(Operation)*

- DER *(Detection and Reaction)*

The system-oriented modules are grouped into the following layers:

- INF *(Infrastructure)*
- NET *(Networks and Communication)*
- SYS *(IT Systems)*
- APP *(Applications)*
- IND *(Industrial IT)*

Every module includes a short description of the topic and the goal to be achieved by implementing the module, as well as a differentiation regarding other modules that are related with regard to their topic. Moreover, there is a short overview on the specific risks of the considered topic. The main part is made by the concrete security requirements for Basic Protection, Standard Protection and Core Protection.

In addition, there can be implementation recommendations for the modules of the IT-Grundschutz Compendium. They describe how the requirements of the modules can be met in practice, and they include corresponding security safeguards with detailed descriptions based on the experiences of BSI and IT-Grundschutz users.

2.5 Scope of the subject area

The goal of information security is to protect information. This information might be stored on IT Systems, but also on paper or inside people's heads. IT security primarily concerns protecting and processing information stored electronically. In case of cyber security, the field of action of classic IT security is extended to the whole cyberspace. This comprises any and all information technology connected to the Internet and comparable networks, and includes communication, applications, processes and processed information based on the aforementioned. Thus, the term “information security” instead of IT security or cyber security is more comprehensive. IT-Grundschutz has long been pursuing a holistic approach that also offers protection for business information and business processes not supported or only supported in part by IT. However, since the term "IT security" is still overwhelmingly used in the literature, it will still be used in this and other publications relating to IT-Grundschutz, although the documents will place more and more emphasis on considering information security over time.

The objective of information security is to provide appropriate protection of the basic values of confidentiality, integrity (genuineness) and availability of information. This also includes securing of information processing, i.e. particularly of IT. Moreover, the systems that often are not directly considered to be IT systems, e.g. ICS and IoT systems, also must be included. Furthermore, this also includes authenticity and non-repudiation as special cases of integrity. Depending on the application case, it can be useful to consider further basic values. In the field of data protection, further protection goals are considered within the scope of the standard data protection model (see [SDM]), i.e. data minimisation, intervenability (as a technical form of methods for exerting rights of individuals affected), transparency and non-concatenation (for securing purpose limitation).

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. Some BSI documents still use the term "IT security management" instead of information security management (or the abbreviated form IS management) for the same reasons as mentioned above for the terms "information security" and "IT security".

2.6 Overview of the information security process

The IT-Grundschutz approaches provide 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 solutions to special problems.

In order to achieve an appropriate level of security a systematic approach is required for designing the security process. As defined by IT-Grundschutz, the security process is comprised of the following phases:

- Initiation of the security process
  - Acceptance of responsibility by the management level
  - Designing and planning the security process
  - Provision of financial resources, personnel, and the necessary time
  - Deciding on an approach
- Drawing up of an information security policy
- Establishment of a suitable organisational structure for information security management
- Drawing up of a security concept
- Implementation of the security concept
- Maintenance and continuous improvement of information security
  - Further development of ISMS
  - Extension of selected approach

Holistic implementation of information security (Standard Protection) in a single large step is frequently too ambitious. Many small steps and a long-term, continuous process of improvement without high initial investment costs often bring greater success. Thus, it could be better initially to only implement the urgently required security safeguards (Basic Protection) or to rapidly reach the required high level of security in areas with the highest security requirements (Core Protection). The security of the whole organisation can then be continuously improved from these starting points.

Those responsible for information security can use the IT-Grundschutz approaches and IT-Grundschutz Compendium for various reasons and objectives. Therefore, the order and intensity of the individual phases varies with the existing security environment and the user's perspective. For example, regular revision of the security concept often sets other focuses as compared to integration of new business processes.

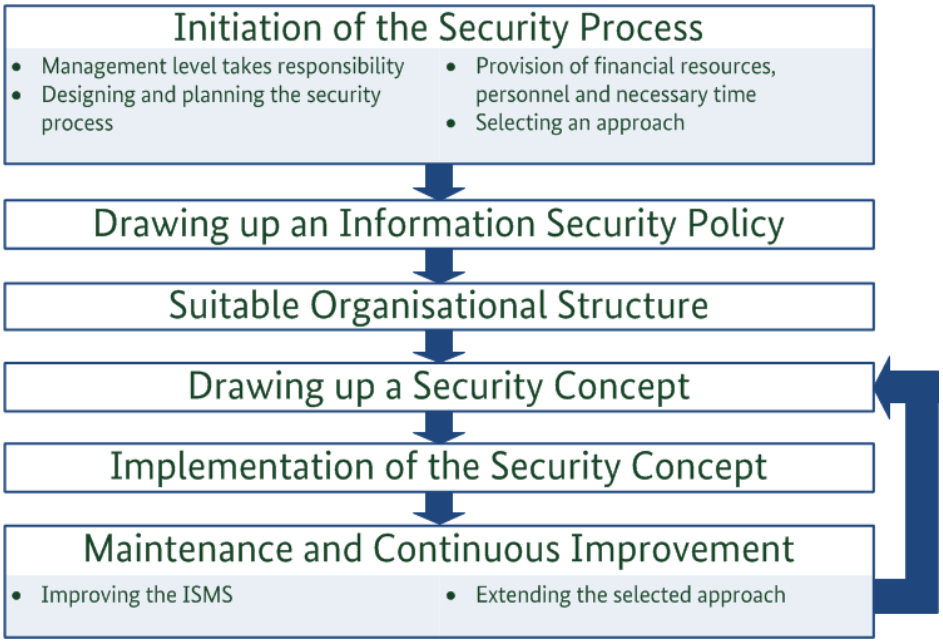


Figure 1: Phases of the security process

Some of the phases can also be performed in parallel, e.g. designing and planning the security process can be done simultaneously with creation of the information security organisation. In this case the advance phases must be updated later to take the new results into account.

The following provides a short presentation of the phases of the security process.

Initiation of the security process

The management level must initiate, control and monitor the security process. This requires strategic guiding statements regarding the information security, on the one hand, and general organisational conditions, on the other. The structure of a functional security process and reasonable organisational structures for this are described in Section 3.

Drawing up of an information security policy

The policy for information security is an essential basis for the design of the security process. It describes the security goals and level of security pursued by the organisation, the motivation for this, and the safeguards and structures used to achieve this. Therefore, all employees should know and understand the content of the security policy. Section 3.4 describes what is to be considered for the policy and other documents in the security process.

Design of a suitable organisational structure

Information security management requires establishment of an organisational structure that is suitable for the size and type of the organisation, see Section 4.

Drawing up of a security concept

After initiating an information security process and defining the security policy and information security organisation, the organisation's security concept is worked out. As a basis for this, the modules of the IT-Grundschutz Compendium include corresponding state-of-the-art security requirements for typical components of business processes, applications, IT systems and other objects. Based on their topic, these are classified into modules so that they can build on each other.

The individual activities for drawing up of a security concept slightly differ depending on whether Basic Protection, Standard Protection or Core Protection is intended; however, in principle they are all based on the preliminary work performed with drawing up of the IT-Grundschutz Compendium.

When employing IT-Grundschutz, a gap analysis between the security requirements of the relevant modules of the IT-Grundschutz Compendium and the safeguards already used at the organisation is performed. Requirements that are found to be missing or inadequately fulfilled reveal security deficits that can be rectified by implementing the safeguards derived from the requirements.

Only if the protection requirements are significantly higher, it will be necessary to also perform a risk analysis, weighing up the cost-effectiveness of implementing additional safeguards. Usually, it will be sufficient here to add corresponding individual, higher-quality safeguards to the security requirements of the IT-Grundschutz Compendium. In this regard, BSI-Standard 200-3 *Risk Analysis based on IT Grundschutz* (see [BSI3]) describes a simpler methodology as compared to traditional risk analysis methods.

Implementation of security concepts

A sufficient level of security can only be achieved if existing deficits are determined, the status quo is recorded in a security concept, required safeguards are identified, and these safeguards particularly are implemented in a consequent manner. Section 9 describes the factors which should be considered when planning the implementation of security safeguards.

Maintenance and continuous improvement of information security

The goal of security management is to reach the desired level of security and to permanently maintain and improve it. Therefore, the security process and the organisational structures for information security shall be checked at regular intervals for their adequateness, effectiveness and efficiency. It shall also be checked if the safeguards of the security concept still fit the information domain, if they

are practical and if they were implemented correctly. Section 10 shows an overview of the actions that should be performed for maintenance and improvement of information security. This also includes considering whether the selected approach should be supplemented or extended, for example from Basic Protection to Standard Protection or from Core Protection of a limited area to a larger information domain.

2.7 Use of the IT-Grundschutz Compendium

After the management level defined the security process on the strategic level by drawing up of the information security policy and creating the information security organisation, such process will be continued on the operative level by using the security concept. Thus, the creation of a security design is one of the primary tasks of information security management. Here, the required security safeguards are identified and documented.

IT-Grundschutz follows a modular approach to enable improved preparation and structuring of the highly heterogeneous designs of organisations of various industries and sizes as well as their employed IT or ICS systems, including the application environment. The individual modules that are described in the IT-Grundschutz Compendium reflect typical areas and aspects of information security within an organisation, from generic issues such as IS management, contingency planning or the data backup concept right up to special components in an IT or ICS environment. The IT-Grundschutz Compendium describes the specific threat scenarios and the security requirements for various components, approaches and systems, which are each consolidated into one module. The BSI, together with many committed users, re-works and updates the existing modules at regular intervals in order to keep the recommendations in line with the latest technological developments. In addition, new modules are regularly added to the existing body of documentation. Users may propose or create modules. Under the leadership of the IT-Grundschutz team of BSI, first they are prepared as a Community Draft into which further suggestions can be integrated, before being included into the IT-Grundschutz Compendium.

The modules play a central role in the IT-Grundschutz Methodology. They are structured in the same manner in order to simplify their use. Every module starts with a short description of the considered component, the procedure and/or the system, including objective, as well as a differentiation regarding other modules that are related with regard to their topic. The specific threat scenario is described after that.

Then, the security requirements, divided into basic and standard requirements as well as requirements in the case of high protection requirements, will follow. Taken together, the basic and standard requirements stated in the IT-Grundschutz Compendium represent the state of the art. These must be fulfilled for certification according to ISO 27001 on the basis of IT-Grundschutz.

In the requirements, the modal verbs “SHOULD” and “MUST” written in capital letters are used in their respective forms as well as in the corresponding negations to make clear how the corresponding requirements are to be interpreted. The definitions used here are based on [RFC2119] as well as DIN 820-2:2012, Annexe H [820-2].

MUST:	This term means that this is a requirement that must be imperatively fulfilled (absolute requirement).
MUST NOT / MUST NO:	This term means that something must not be done in no case (absolute prohibition).
SHOULD:	This term means that a requirement usually must be fulfilled, but that there can be reasons to not fulfil the requirement. However, this must be carefully assessed and well founded.
SHOULD NOT / SHOULD NO:	This term means that something should not be done usually, but that there can be reasons to do it. However, this must be carefully assessed and well founded.

Security concepts that have been produced with the aid of IT-Grundschutz are compact because, in the concept, it is simply necessary to make a reference to the relevant security requirements in the IT-Grundschutz Compendium. This promotes understandability and clarity in the concepts. For simplification of implementation of the security requirements, there are additional implementation recommendations for many modules of the IT-Grundschutz Compendium. They describe how the requirements of the modules can be fulfilled in practice, and they include corresponding security safeguards with a detailed description. When technical terminology is used, it is ensured that the descriptions can be understood by those who need to implement the safeguards. It should be noted that the implementation recommendations represent an assistance for fulfilment of the requirements of the corresponding modules and no binding specifications.

Note: The comprehensive information regarding IT-Grundschutz do not substitute common sense. Understanding, implementing and living information security should be top priority. The IT-Grundschutz Compendium provides a lot of information and recommendations for many aspects. When they are processed, it should always be considered that the security requirements suitable for the corresponding organisation and their framework conditions are selected from these and adapted. Additional information on adapting module requirements are included in Section 8.3.6. Neither the requirements of the modules of the IT-Grundschutz Compendium, nor the safeguards of the implementation recommendations should be used as mere check lists for status determination, but should be adapted realistically to the individual conditions.

In order to simplify the implementation of the safeguards, the IT-Grundschutz texts are also provided consistently in electronic form. In addition, implementing the security requirements and safeguards is also supported via auxiliary materials and sample solutions that are provided in part by the BSI and in part by IT-Grundschutz users.

3 Initiating the security process

Achieving and/or maintaining an appropriate and sufficient level of information security in the organisation requires a *planned approach* on the one hand and an *adequate organisational structure* on the other hand. Furthermore, it is required to define *security objectives* and a *strategy for achieving* such objectives as well as to finally establish a continuous security process for maintenance of the level of security reached so far. Because of the high importance, the far-reaching consequences of the decisions made and the high responsibility, this issue must be initiated by the highest level of management.

3.1 Accepting responsibility by management

The top management level in each public agency and company is responsible for the proper, goal-oriented operation of departments and for early detection and minimisation of risks. Given the increasing dependence of business processes on information processing, there is also an increase on the requirements on ensuring information security both internally and externally.

The top management level must initiate, control and monitor the security process. The management level is the instance that takes decisions on handling risks and must provide the relevant resources. The responsibility for information security remains on such level. However, the operative tasks of "information security" usually is delegated to an information security officer (ISO).

In the introductory phase of the security process, it is quite often the case, that no security organisation has been established and the later ISO has not been appointed yet. However, initiation of the security process requires appointment of a person responsible for information security performing the first steps for designing and planning the entry into information security.

After a security incident, the management of a company or public agency may consider early provisioning of information on possible risks when handling information, business processes and IT to be an obligation to be provided by the IT and security experts. For this reason, it is recommended that those person being in such roles verifiably inform the top management level about the potential risks and consequences of a lapse in information security. However, management is also responsible for ensuring that they receive any decision-relevant information in good time and with the appropriate scope. The issues relating to security include:

- the security risks for the organisation and its information as well as the related effects and costs,
- the impact of security incidents on critical business processes,
- the security requirements resulting from statutory or contractual stipulations,
- the standard information security procedures typical for the industry,
- the current state of information security regarding a level of maturity and correspondingly derived recommendations for action.

Although management is responsible for achieving the security objectives, all the organisation's employees must be involved in the security process.

Above all, the management must ensure that information security is integrated into all relevant business processes, specialised procedures and projects. Experience has demonstrated that the ISO requires the full support of management in order to be integrated into each key activity by the person responsible due to the pressure to perform that exists everywhere.

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

Action points on 3.1 Accepting responsibility by management

- The management level is informed regularly on possible risks and consequences of a lack of information security.
- The management level accepts overall responsibility for information security.
- The management level initiates the information security process within the organisation and appoints a person responsible for information security.

3.2 Designing and planning the security process

It is necessary to establish a continuous information security process and to define an appropriate strategy for information security (IS strategy) to be able to achieve and maintain an appropriate level of security. This is useful for planning of further procedure to achieve the security objectives set. It is decided by the management and is based on the company's business objectives or the role of a public agency. The management stipulates the basic security objectives and the level of information security that is appropriate for the business objectives or specialised tasks. Management must also provide the funds required.

3.2.1 Determining the framework conditions

All relevant framework conditions must be identified to define an appropriate IS strategy. Thus, every organisation should determine its most important business processes and specialised tasks as well as its need for information security. This also includes analysis of stakeholders (i.e. the relevant internal and external parties), business objectives, tasks and their requirements regarding security. The connections between business processes and the information processed there as well as the employed information technology form the basis for the decision on which level of security is appropriate for protection of information and for information technology, respectively.

Determining framework conditions is an essential basis for further considerations of information security as this may identify places with lack of background information for being able to correctly assess the importance of information security for the organisation. Moreover, this enables first self-assessment as it becomes evident during compilation of background information already where there is a potential for conflict and where activities are required.

General influencing factors

Information security helps the organisation to achieve their business goals. Thus, the influencing factors derived from this must be considered:

- Business goals: Which factors are essential for success of the company or public agency? Which products, offers and orders form the basis of the business activities? What are the general goals of the organisation? Which role does information security play in this regard?
- Organisational structure: How is the organisation organised and structured? Which management systems are present (for example, risk management or quality management)?
- Cooperation with externals: What are the most important internal and external customers, partners and influencing bodies? What are their basic requirements and expectations regarding information security of the organisation? What are the most important service providers and suppliers? What is their role for the organisation’s information security?
- Strategic context: What are the main challenges for the organisation? How is the competitive position? How does this affect the risk appetite of the organisation and the handling of information security?

Internal framework conditions

Many internal conditions may affect information security, and these must be determined correspondingly. The analysis of business processes and specialised tasks provides statements about the effects of security incidents on the business activity and the fulfilment of tasks. At this early stage

it is not important to describe the information technology in detail. There should be a basic summary of which information is processed for a business process with which IT applications and systems.

Often the organisations already have summaries of business processes, objects and data collections required for operational aspects or administration. If they exist, available process maps, business distribution plans, databases, summaries, network plans and inventory tools can be used to identify the essential business processes. If such summaries are taken into account, it should be ensured that the level of detail of the collection does not become too deep so that the extent for first overview and as basis for later decisions will not become too comprehensive.

The following aspects should be considered:

- Which business processes are present in the organisation, and how are they connected to the business goals?
- Which business processes depend on functional information technology, i.e. IT that meets the requirements and operates properly?
- Which information is processed within scope of these business processes?
- Which information is particularly important and, correspondingly, is worthy of protection with regard to confidentiality, integrity and availability, and why? Examples include personal data, customer data, strategic information or secrets such as development data, patents, process descriptions.
- A responsible contact person must be appointed for each business process and specialised task; this person acts as the so-called "information owner" for all issues relating to processing data within this business process.

External framework conditions

In addition, all external framework conditions having an impact on information security must be determined, such as

- legal framework conditions (national and international laws and regulations),
- requirements of customers, suppliers and business partners, current market situation, competitive situation and further relevant market-specific dependences,
- industry-specific security standards.

Brainstorming

In order to determine the relevant conditions for each key business process as quickly and in as much detail as possible, it is advisable to hold a short security meeting (brainstorming) for each business process. The security meetings should be led by the ISO with the relevant information owners or specialists responsible and the relevant person responsible for IT. Size and complexity of the organisation define whether one or several meetings will be required.

Primarily, business-critical information and core processes should be determined and the corresponding applications, IT systems, networks and rooms should be identified. Here, the essential supporting processes and the mainly affected objects should be determined on the basis of the core processes of the organisation. It has become apparent that it is difficult to consider abstract processes separately from concrete technical components. Thus, optionally it can be reasonable to not only determine the assets from a process view, but also to determine, from the view of known assets, the processes that use such assets. Such optional procedure will be particularly reasonable if no complete process map is available and the management experience difficulties in defining such process map.

Participation of the level of management in the brainstorming is not mandatory. However, it is much more important that each participant is capable of providing information on the area represented by such participant, and that such participant is able to name the essential business processes of the own area as well as the employed assets. Usually, the initial process should not be longer than half a day.

The results should be documented in line with a pre-set scheme and reported to the level of management.

3.2.2 Formulate general information security objectives

The information security objectives should be determined carefully at the start of each security process. Otherwise, there is a risk that the security strategies and concepts worked out will not match the actual requirements of the organisation.

Therefore, general security objects should first be derived from the organisation's fundamental objectives and the general environment. Specific security requirements for handling of information and 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 such items as:

- high reliability for actions, and for handling information in particular (availability, integrity, confidentiality),
- ensuring the good reputation of the organisation in the eyes of the public,
- preserving the value of investments in technology, information, work processes and knowledge,
- protecting the high and possibly irretrievable value of information processed,
- satisfying the requirements resulting from statutory provisions,
- protection of natural persons regarding their physical and mental integrity.

In order to be able to define the security objectives, estimates should first be made on which business processes, specialised procedures and information are essential to meet the objective and which value these are assigned. Here it is important to make clear how strong the fulfilment of tasks within the organisation depends on confidentiality, integrity and availability of information and on the employed IT and its secure functioning. In order to define the security objectives, it is appropriate to expressly state the basic protection values – availability, integrity and confidentiality – and possibly to prioritise them. These statements play a key role throughout the security process when selecting security safeguards and strategies.

No detailed analysis of the information domain and the potential cost of security safeguards is required at this point; all that is required is a statement on what is of particular importance to the organisation and why.

3.2.3 Determining the appropriate security level of the business processes

In order to better understand the information security objectives, the desired security level can be described for individual business processes or organisational areas of particular interest with reference to the basic values of information security (confidentiality, integrity, availability). This is valuable for stipulating the detailed security concept later.

The following are some sample criteria for determining an appropriate level of security. The security level (normal, high or very high) of individual business processes and/or areas can be determined by the statement that fits most closely. This phase of the security process concerns stipulating the initial statements that will be used later as the foundation, and not about defining the protection requirements in detail.

Very high:

- The protection of confidential information must be guaranteed and comply with strict secrecy requirements in critical areas. Disclosure of particularly critical or highly confidential information may have a serious impact of further existence of the organisation.
- It is critically important that the information is correct.

- The central 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 not acceptable.
- Protection of personal data must be ensured imperatively. Otherwise, there may be a danger to life and limb or to the personal freedom of the affected person.

The following generally applies: Failure of the IT or essential business processes or disclosure and/or manipulation of critical information leads to collapse of the organisation or has serious consequences for large parts of society or industry.

High:

- The protection of confidential information must be guaranteed and comply with strict secrecy requirements in critical areas.
- The information processed must be correct; any errors must be detectable and avoidable.
- In central areas of the organisation time-critical processes are undertaken or mass tasks are undertaken that could not be completed without the use of IT. Only very short downtime is acceptable.
- Protection of personal data must meet high requirements. Otherwise, there is the risk that the social or financial standing of those concerned will be seriously impaired.

The following generally applies: In the event of damage, key areas of the organisation can no longer function; the result of damage is significant disruption of the organisation or affected third parties.

Normal:

- The protection of information only intended for internal use must be ensured.
- Information should be correct. Smaller errors can be tolerated. Errors that substantially affect the fulfilment of objectives must be recognisable or avoidable.
- Extended periods of downtime which lead to deadlines being missed cannot be tolerated.
- Protection of personal data must be ensured. Otherwise, there is the risk that the social or financial standing of those concerned will be impaired.

The following generally applies: the result of damage is disruption of the organisation.

Note:

Every organisation should adapt the formulations to its individual situation. It can also be reasonable to define further categories, e.g. to for example make upward and downward delimitations more distinct. The security objectives also reflect the present security culture within an organisation, i.e. how security risks and safeguards are dealt with.

The involvement of management is essential in stipulating information security objectives. To determine the desired level of security, the organisation's objectives must be viewed with reference to the security requirements whilst taking into account that there are usually limited resources available for implementing security safeguards. This is why it is particularly important to identify the actual requirement for availability, integrity and confidentiality because a high level of security is usually related to a high cost of implementation. Furthermore, it is recommended to prioritise the formulated requirements if this is possible already at such point in time.

Notes on the depth of the description

This early stage of the information security process does not involve viewing all the applications and IT systems in detail nor a comprehensive risk analysis. It is important to have an overview of the security requirements made on the information technology due to 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 are particularly critical for the organisation regarding confidentiality, integrity and availability?
- What critical tasks within the organisation cannot be performed at all without IT support or can only be partially performed or with considerable additional effort?
- What effects can deliberate or unintentional security problems have?
- Are the IT assets used to process information which requires particular protection due to its confidential nature?
- What essential decisions made within the organisation rely on the confidentiality, integrity and availability of information and IT systems?
- What organisational or legal requirements (e.g. data protection) result in particular safeguards?

The descriptions of the desired level of security should be adapted to the relevant environment. Brief reasons are helpful for encouraging the activities that are built on them. For example, for a hospital this could mean: "A high level of information security is essential in the x-ray department because human life depends on the correct operation of the IT systems."

3.2.4 First acquisition of processes, applications and IT systems

The results of the previous steps, i.e. determination of framework conditions, formulation of information security objectives and determination of the appropriate security level of the business processes should be consolidated next in an overview of the available assets of the organisation.

Such overview serves as an aid to making a decision for selection of a suitable procedure and is the basis for later steps such as selection of the relevant IT-Grundschutz modules for Basic Protection or structural analysis for Standard Protection. Here, first acquisition of the processes, applications and IT systems should be complete to such an extent that it can be used as an aid to making a decision for selection of the suitable approach for securing the organisation; however, it is not nearly as comprehensive as the result of a structural analysis.

First acquisition provides an overview that can be created in a comparably fast and resource-saving manner. The structural analysis to be performed with Standard Protection can be based on this and provides a more complete picture of the information domain to be secured.

Based on the essential business processes and specialised procedures, first acquisition must include identification of the applications, IT systems, network components, rooms and similar objects that are essential for performance of the business processes. Here, not only the primary dependences should be considered, but also the applications and IT systems directly required for a business process. Also secondary dependences, i.e. the critical support processes and/or systems (such as building services, logistics etc.), should be considered.

If possible, at this point in time it should be assessed whether the identified objects require a higher security level than “normal”.

Here, often it is not reasonable to acquire every object individually, because information domains mainly consist of many individual objects. Instead, similar objects should be reasonably combined in groups. It can also be easier for first acquisition to create a graphical network overview in a second step and to use it as a basis for acquisition of the IT systems. Here, completeness or form is not important. The goal is to get a highly simplified network overview.

First acquisition should also only include the essential objects and not every single IT component. For example, first acquisition should not include typical office rooms; however, server rooms with their special and mainly higher security level should be included.

Acquisition of the relevant objects

Based on each business process and/or each specialised task included in the information domain, the following objects should be acquired by means of a table with unique identifier and at least the following notes:

- Business process or specialised task: Name and (if needed) description, responsible specialised body
- Application: Name, (if required) description and corresponding business process
- IT, ICS systems and other objects: Name, platform and, if reasonable, place of installation
- essential rooms for maintenance of operation correspondingly requiring a higher security level (e.g. data centre, server rooms): Type, room number and building

Virtual IT systems and networks should be treated like physical structures, but should be reasonably identified.

Assessment of security level

Regarding later considerations, it can be reasonable to assess the intended security level of the individual assets already at an earlier point in time. However, the actual determination of the required protection should be performed at a later point in time. Such assessment of the security level provides basic orientation regarding the efforts to be expected and simplifies suitable group formation of the identified assets.

The objects identified so far, for which a higher security level than “normal” is intended, should be identified in the already created table.

Creating a graphical network plan

A rudimentary network plan should be created as an overview on the basis of the acquired information. If an up-to-date network is available, this can be used. A network plan is a graphical representation of the components used in the information and communications technology under consideration and of the manner in which they are networked together. Contrary to a complete or simplified network plan, like it will be created during future structural analysis later on, such network summary serves as an overview simplifying further discussion and showing if essential IT systems have been left out. In detail, the plan should show at least the following objects with regard to information security:

- IT systems, i.e. clients and servers, active network components
- Network connections between such systems
- Outward connections of the considered area

However, the graphical network summary should not be limited to physical components, but should also include virtualised structures. Here, either virtual structures (suitably identified) can be inserted directly into the graphical network summary, or they can be entered into a separate network summary in case of confusing architectures.

An example of first acquisition including a network summary can be found in the resources for IT-Grundschutz. The results obtained here will be clarified and completed within the scope of the structural analysis to be performed later on.

Action points on 3.2 Designing and planning the security process
• Appoint contact persons for all business processes and specialised tasks
• Perform basic assessment on the value and the security level of information, business processes and specialised tasks
• Determine internal and external framework conditions

- Estimate the importance of business processes, specialised tasks and information
- Set general information security objectives
- Create a consolidated summary of the present assets based on the knowledge gained previously
- Obtain the agreement of management

3.3 Decision on approach

IT-Grundschutz offers various approaches intended for different user groups and having different objectives: Basic Protection, Standard Protection and Core Protection. In this step, selection of the optimal approach for the organisation is made on the basis of the already present aid to making a decision, also using the first acquisition performed above.

Basic Protection is a basic safeguarding of the business processes and resources of an organisation. It enables initial entry into the security process to lower the highest risks as fast as possible. In the next step, the actual security requirements can be analysed in detail. Thus, this approach is particularly suitable for smaller organisation being still at the beginning of their security process.

Core Protection serves as further entry approach for protection of the essential business processes and resources of an organisation. This approach differs from the classical IT-Grundschutz by focusing on a small, but very important part of the information domain, the so-called crown jewels. Above all, Core Protection is suited for organisations having identified a few business processes that are essential for the existence of the organisation and require preferential protection.

Standard Protection is the third approach and also preferred by BSI. Basically, this corresponds to the known and proven IT-Grundschutz approach.

Basic Protection and Core Protection are methods to be able to identify and implement the most important security recommendations for the selected field of use in a timely manner, respectively. The objective is to create a complete security concept in accordance with Standard Protection on the medium term.

3.3.1 Basic Protection

The objective of Basic Protection, as start on IT-Grundschutz, primarily is to get a broad and basic initial safeguard of all relevant business processes and/or specialised procedures of an organisation. Such approach is recommended for organisations that meet the following:

- Implementation of information security has only just begun, i.e. information security has only achieved a lower maturity level so far.
- The business processes do not show a significantly increased risk potential regarding information security.
- The intended security level is normal.
- There are no assets whose theft, destruction or compromising will result in a damage that threatens further existence of the organisation.
- Minor security incidents can be tolerated, i.e. incidents that cost money, but do not cause any other damage, and that do not threaten the existence of an organisation when summed up.

Basic Protection first enables implementation of the most important security requirements in a timely manner so that this can be taken as a basis to further increase the security level at a later point in time, e.g. by protecting all areas by using Standard Protection or by protecting critical business processes by using Core Protection.

3.3.2 Core Protection

Core Protection can be used by an organisation as entry into IT-Grundschutz and/or the security process to preferably protect business processes and assets with a particular risk. This approach is recommended if an organisation largely meets the following criteria:

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

Core Protection can be used to protect the most important resources and business processes in a timely manner. Thus, the critical business process can be protected in a first step, to selectively protect the next critical business processes during further steps or start Basic Protection or Standard Protection for all areas of the organisation. Certification according to ISO 27001 is generally possible for the considered delimited information domain.

3.3.3 Standard Protection

The Standard Protection essentially corresponds to the classic IT-Grundschutz approach. Standard Protection can be used to comprehensively and deeply protect an organisation. Basically, this should be the objective of every application of IT-Grundschutz, even though one of the two approaches stated above had been selected previously. Direct entry into the security process by using the Standard Protection will be recommended if the following mainly applies to the organisation:

- The organisation already uses IT-Grundschutz.
- Security concepts have been created already in accordance with IT-Grundschutz or ISO 27001.
- The implementation of information security has reached a sufficient degree of maturity in the organisation, so that security safeguards already exist in key areas and no basic initial safeguards are required.
- There is no need for action to preferentially protect individual business processes having a significantly higher risk potential regarding information security (see Core Protection).
- The organisation does not have assets whose theft, destruction or compromising may result in damage that immediately threatens the existence of the organisation, and who correspondingly require preferential protection.
- Security incidents that perceptibly affect the performance of tasks, cost money or otherwise result in damage are not acceptable for the organisation even if they do not cause a damage that threatens the existence of the organisation.

Standard Protection is the approach that generally should be aimed at to properly and comprehensively protect all areas of an organisation. Such approach (and/or the Core Protection) is the required basis for any intended certification of the information domain in accordance with ISO 27001.

3.3.4 Specification of the scope

The scope for drawing up of the security concept will be referred to as “information domain” in the following. An information domain comprises all the infrastructural, organisational, personnel and technical components which serve to perform tasks in a particular field of information processing. An

information domain may comprise to the entire information processing of an organisation or to individual areas defined by organisational or technical structures (e.g. department network) or joint business processes and/or shared applications (e.g. HR information domain).

In addition to the approach, also the design of the information domain to be protected with it must be defined. This may include the whole organisation or just parts. For example, certain organisational units of an organisation can be considered to be an information domain. However, this can also be areas processing defined business processes, including the correspondingly required infrastructure. It is important, though, for the scope to include all business processes examined.

Whilst the scope often includes the whole organisation in case of Basic Protection and Standard Protection, in case of Core Protection the focus will be on some outstanding processes that are critical for the business.

It can also be reasonable to develop security concepts for several smaller areas. This can be the case e.g. if the efforts for overall safeguard during the first step are considered to be too high and certain business processes require prioritised treatment. For example, areas for which Basic Protection, Standard Protection and/or Core Protection has been performed in parallel or successively could be identified for this.

Thus, an organisation could decide to first implement Core Protection for a small area with assets having a particular risk. However, Basic Protection should be ensured for the rest of the institution so that there will be a minimum security.

When delimiting the scope, not only the technical, but also organisational aspects should be considered so that the responsibility and competences can be clearly defined. In any case it should be clear which information, specialised tasks or business processes are explicitly considered in the security concept.

When delimiting the scope for the security concept, the following factors should be considered:

- If possible, the scope should comprise all areas, aspects and components which serve for supporting the specialised tasks, business processes or organisational units and which are administrated within the organisation.
- If this is not possible, because the organisation of parts of the specialised tasks or business processes considered depends on external partners, for example, within the scope of outsourcing, the interfaces should be clearly defined, so that this can be taken into account within the scope of the security concept.

Action points on 3.3.4 Definition of the scope for the security concept
• Define which critical business processes, specialised tasks or parts of the organisation should be included in the scope • Clearly delimit the scope • Describe interfaces to external partners

3.3.5 Management decision

Based on the determined framework conditions, the formulated security objectives and the intended security level, the person responsible for information security as appointed by the level of management must elaborate a proposal on how the further steps for achieving the short-term and long-term security objectives should look like. The management should take this as a basis for deciding on which approach is to be selected for which areas of the organisation for their corresponding protection.

Then it should be documented for which area and with which schedule a Basic Protection, Standard Protection and/or Core Protection should be implemented. The corresponding scopes of the information domain should be defined.

The following overview shows the most important pros and cons of the individual approaches.

Basic Protection

Pros The efforts are relatively low. This enables quick entry into information security. Thus, basic initial safeguard can be achieved quickly.

Cons There is only a low security level due to general fulfilment of the first requirements. Possibly, the achievable protection level is not sufficiently high for the actual security requirements. Certification in accordance with ISO 27001 is not possible on this basis.

Core Protection

Pros Core Protection enables complete focussing on the crown jewels, i.e. the assets that are existentially important for the organisation. Implementation is faster than with inclusion of all business processes. Certification according to ISO 27001 is generally possible for the considered delimited information domain.

Cons It is possible that crown jewels cannot be considered separately so that more comprehensive parts of the organisation must be integrated. The business processes classified as being non-critical are not regarded initially. On the one hand, there will be the risk that important areas will be disregarded and correspondingly will be completely unprotected. On the other hand, cumulated risks can be overlooked.

Standard Protection

Pros Standard Protection offers a high security level specifically adapted to the present business processes. A uniform security level for the whole organisation is achieved. The achieved security level can be well compared to levels of other organisations. Certification in accordance with ISO 27001 and measurability of ISMS are possible. All required resources of the organisation are fully considered.

Cons The efforts on a lower maturity level of the present information security are higher as compared to other approaches.

Action points on 3.3.5 Management decision
• Elaboration of a management submittal for decision-making
• Decision on which approach is to be selected for which areas of the organisation for their corresponding protection
• Documentation of decision and time schedule for implementation

3.4 Drawing up a policy for information security

The policy on information security describes in general terms how information security is to be established in the organisation, for which purposes and with which resources and structures. It contains the information security objectives aimed at by the organisation and the information security strategy pursued. The security policy therefore also describes the level of security aimed at in a government agency or company beyond the security objectives. It is therefore both a requirement and a statement that this level of security should be obtained at all levels within the organisation.

The preparation of the security policy should be achieved via the following steps:

3.4.1 Responsibility of management of the public agency and/or company for the security policy

The policy on information security documents the strategic position taken by management and administration to achieve the information security objectives throughout the organisation.

Since the security policy represents a central strategy paper for information security in an organisation, it must be designed such that all addressed organisational units can identify with its

content. Therefore, as many departments as possible should be involved in its preparation. After all, each organisation must ultimately decide which departments and hierarchical levels will be involved in formulating the security policy.

When preparing an security policy, it is advisable to use the expertise of the following organisational units: Specialised persons for important applications, IT operations, security (information, IT and infrastructure security), data protection officer, production and manufacturing, HR, personnel representative, auditing, representative for finances, legal department.

3.4.2 Convening a team responsible for developing the security policy

If an IS management team already exists within the organisation, then this should be responsible for developing and/or reviewing and re-working the information security policy. The draft document is then submitted to the administration and management, respectively, for approval.

If the information security management is being established for the first time, then a development team should be established to draw up the security policy. This group can assume the function of the IS management team during the security process. It is advisable for this development team to include representatives of the IT and/or ICS users and the IT and/or ICS operational team plus one or more additional employees who already possess sufficient knowledge and experience in matters of information security. Ideally, a member of management who is able to assess the importance of information processing to the organisation should be called in from time to time.

3.4.3 Specification of the scope and the content 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, however, important that the business tasks and processes under review are completely included in the scope. Stipulating the scope is not a trivial tasks, in particular for larger organisations. Organising this by areas of responsibility can be helpful.

The security policy should be formulated clearly and briefly, because more than twenty pages have not been successful in practice. It should contain the following information as a minimum:

- value of information security and importance of the essential information, business processes and IT systems for performance of tasks,
- reference of information security objectives to the objectives or tasks of the organisation,
- security objectives and the key elements of the security strategy for the business processes and IT used,
- assurance that the security policy is implemented by the organisation management, as well as key statements on monitoring success, and
- description of the organisational structure established for implementation of the information security process.

In addition, the following statements may be added:

- For motivational reasons, some threats that are important to the business processes may be sketched, and the most important statutory regulations and other important conditions (such as contractual agreements) may be stated.
- The essential tasks and competences in the security process should be shown (in particular for the IS management team, the IS officer, the members of staff and the IT operations; detailed information on the individual roles are included in Section 4 “Organisation of the security process”). Furthermore, the organisational units or roles acting as contact persons for security questions should be named.
- Programmes to promote information security via training and awareness-raising activities may also be announced.

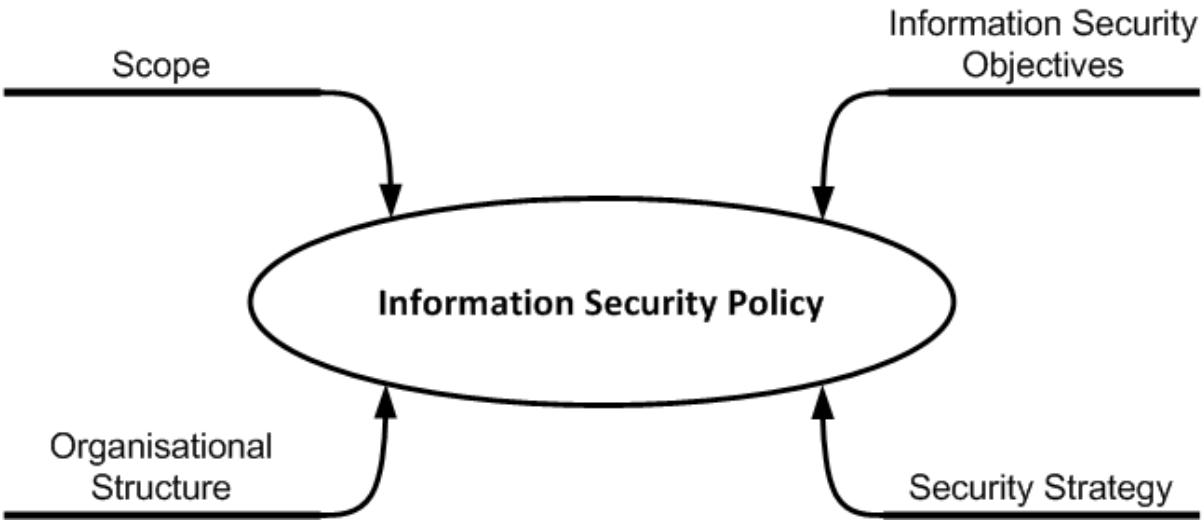


Figure 2: Content of the security policy

3.4.4 Notification of the security policy

It is important that the administration or management underlines its objectives and expectations through publishing the security policy and emphasizes the value and importance of information security throughout the whole organisation. Therefore, all employees should know and understand the content of the security policy. The security policy should be explained to new employees before they receive access to information processing.

As the administration or management has ultimate responsibility for the security policy, the policy should be set down in writing. The document must be formally approved by the administration or management. The content of the security policy should not only be known within the organisation but also be as easily accessible as possible, e.g. on the Intranet of the organisation. If the policy contains confidential statements, they should be located in an appendix that is clearly marked "confidential".

Finally, all members of staff should be made aware of the fact that commitment, co-operation and responsible behaviour are 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.

3.4.5 Updating of the security policy

The policy for information security should be checked and updated if necessary at regular intervals. For example, consideration should be given as to whether business objectives, tasks and therefore business processes or IT procedures or ICS components have changed, whether the organisational structure has been altered or whether new IT or ICS systems have been introduced. As a result of the rapid developments in IT, on the one hand, and the security situation, on the other, it is advisable to revise the security policy at least every two years.

Action points on 3.4 Drawing up an information security policy
• Obtain request from the management to produce a security policy
• Convene a group to develop the security policy
• Specify scope and content
• Organise management approval of security policy
• Announce the security policy
• Regularly check and, if necessary, update security policy

4 Organisation of the security process

The desired level of security can only be achieved if the information security process is implemented for the whole scope. This generic nature of the security process makes it necessary to stipulate roles within the organisation and assign appropriate tasks to these roles. These roles must then be assigned to qualified employees who complete them. This is the only way to ensure that all important aspects are taken into consideration and that all tasks are performed efficiently and effectively.

The organisational structure required to promote and implement the information security process is referred to as the information security organisation or, in brief, IS organisation.

The number of people dealing with information security, the organisational structure and resources vary with the size, type and structure of the respective organisation. In any case, an information security officer (ISO) should be appointed as central contact person for coordination, administration and communication of the information security process. Usually, in larger organisations there are also other persons performing several subtasks of information security. For coordinating their activities, there should also be an IS management team that handles all generic information security issues and works on plans, regulations and policies.

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

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

Basic rules when defining roles in the information security management

- The overall responsibility for the proper and secure provision of tasks (and therefore information security) remains at the management level.
- At least one person (usually the Information Security Officer) is to be appointed to promote and co-ordinate the information security process.
- Each employee is equally responsible for their original task and for maintaining information security in the workplace and in his or her environment.

4.1 Integrating information security into organisation-wide procedures and processes

Information security management is only one of many management tasks, but it influences almost every area within an organisation. Therefore, information security management must be appropriately integrated into the existing organisational structures, and a contact person must be appointed. Tasks and responsibilities must be clearly separated from each other. It must be ensured in this regard that the necessary security aspects are not only taken into account with individual safeguards, but also with all strategic decisions. This includes, for example, decisions on outsourcing or on the use of new electronic distribution channels as well as renting of new rooms. Thus, the IS organisation must be involved in good time in all projects that could affect information security.

In larger organisations in particular, there is often already a global risk management system implemented. As information security risks, in addition to IT risks, belong to the most important operational risks, the methods for information security management and for management of risks should be adjusted to the already established methods and management systems, see also BSI-Standard 200-3 *Risk Analysis based on IT Grundschutz*.

4.2 Creating the information security organisation

Depending on the size of the organisation there are various possibilities for the organisational structure of information security management.

The following diagrams show three of these. The first diagram shows the structure for the IS organisation in a large organisation. The second diagram shows the structure in a medium-sized organisation, where the IS Management Team and the Security Officer are combined. The third diagram shows a structure for the IS organisation in a small organisation, in which the Information Security Officer performs all tasks. The fourth diagram shows a structure of the IS organisation into which an ICS area is integrated.

Moreover, every organisation should appoint a Data Protection Officer (bDSB) in the company and/or government agency. Many tasks are similar; thus, ISO and bDSB should cooperate closely. The bDSB, like the ISO, must have the direct right of recitation at any time with the management of the public agency and/or company.

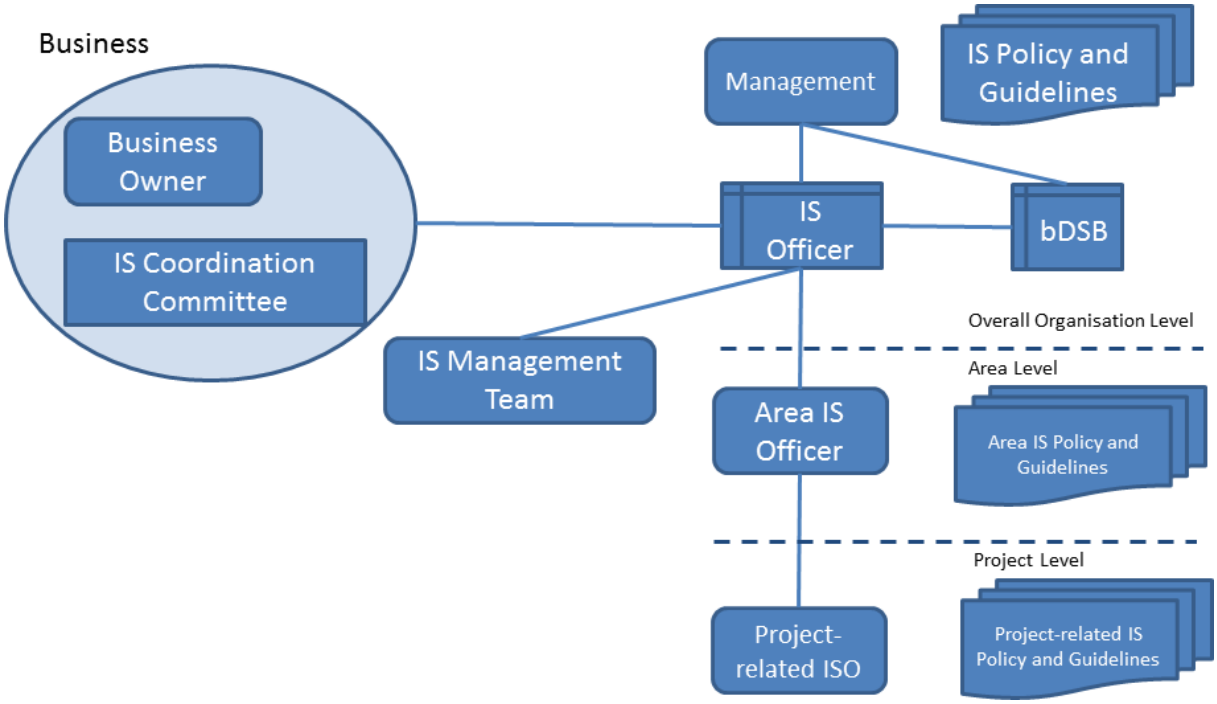


Figure 3: Structure of an IS organisation in a large organisation

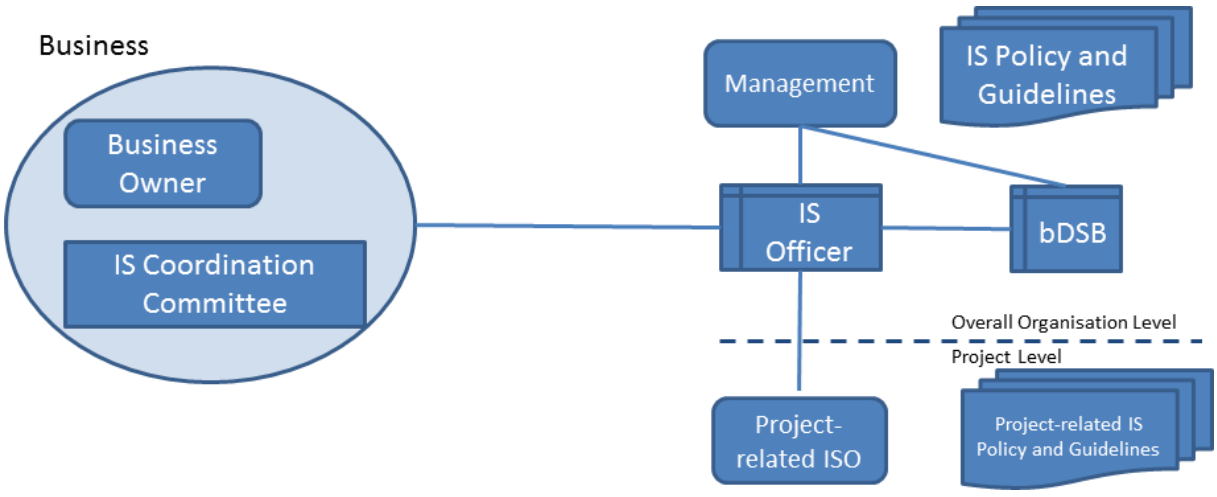


Figure 4: Structure of the IS organisation in a medium-sized organisation

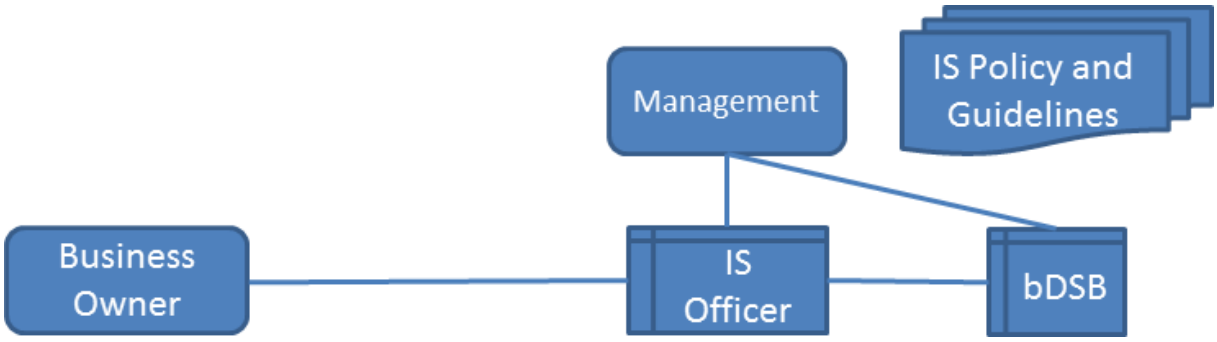


Figure 5: Structure of the IS organisation in a small organisation

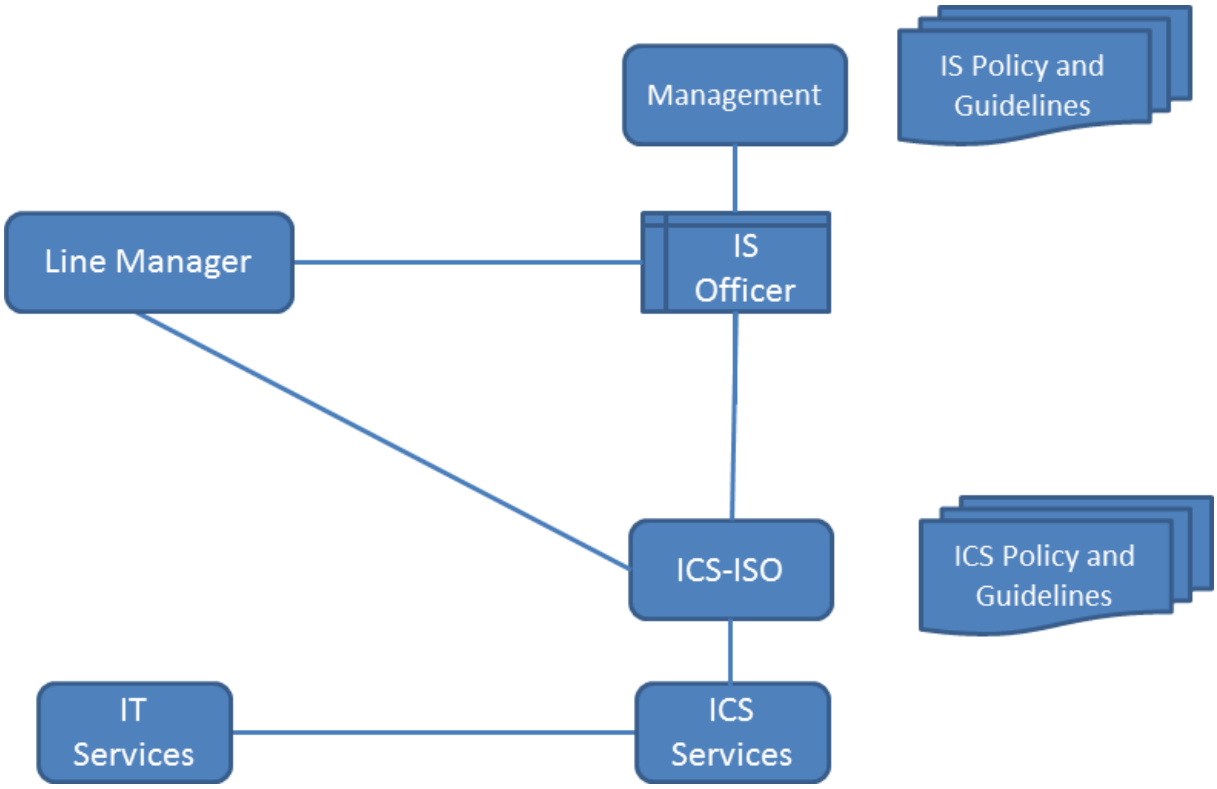


Figure 6: Structure of the IS organisation with integrated ICS area

At this point, it should be clearly emphasised that the central roles shown in these diagrams do not need to be performed by different people. Staffing arrangements should reflect the size of the organisation concerned, the existing resources and the desired level of security. The resources planned for supporting information security must be made such that the agreed level of security can actually be achieved.

4.3 Tasks, responsibilities and competencies in the IS organisation

The Information Security Officer and the IS Management Team must have clearly defined tasks, fields of responsibility, and authorities, which must be laid down by management. In order to be able to perform their tasks, they should both be involved in all relevant procedures and decisions. The roles should be integrated into the organisational structure such that all those involved can communicate with each other. Furthermore, it must be clarified who will communicate when and using which internal and external bodies within scope of security management, as well as which

communication channels are used for the corresponding contact persons and how such channels are protected (see also Section 5.2 *Information flow within information security process*).

The roles of Security Officer and member of the IS Management Team should be entrusted to staff who possess the relevant specialised skills. If necessary, to support these roles, tasks can be delegated to further roles such as

- Area ISO (Information Security Officer for an area, department, connecting branches or similar)
- Project-related ISO as well as
- ICS-ISO (Information Security Officer for the area of Industrial Control Systems).

4.4 The Information Security Officer

Information security is frequently neglected so that it is cut down as compared to day-to-day business. If distribution of responsibilities is not clear there will be a risk that information security becomes "other people's problem". The result is that the responsibility for information security is shifted around until no one takes responsibility for it any longer. To avoid this, a main contact person for all aspects of information security – an Information Security Officer or briefly ISO – should be appointed to coordinate and advance within the organisation the task of “information security”. Whether there are other people who also have security roles and how information security is organised varies with the type and size of the organisation.

The role of the person in charge of information security has different names depending on the type and orientation of the organisation. In addition to Information Security Officer, frequent titles are Chief Information Security Officer (CISO) or Information Security Manager (ISM). Up to now, the IT-Grundschutz documents used the term IT security officer (IT-SiBe) as such term had been the most common term used by companies and public agencies. On the other hand, the title "Security Officer" commonly refers to those persons responsible for industrial safety, employee safety, or plant security.

However, such titles result in a different understanding of the role. For example, using the title Information Security Officer instead of IT security officer makes clear that such person takes care of securing any type of information and not only of IT-related aspects. Information security always should be part of the operational risk management of an organisation. That is why the title Information Security Officer (ISO) replaces the title IT security Officer (IT-SiBe) in IT-Grundschutz in this connection.

This is also closely related to the questions where the security officer is positioned within the organisation. It is recommended to directly allocate the position of the Information Security Officer to the top management level. It is advised to not position the security officer within the IT department as this may result in conflict of roles.

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

Responsibilities and tasks

The Information Security Officer is responsible for managing all the information security issues within the organisation. The main role of the ISO is to advise the administration or management in undertaking their information security roles and to support them in implementing them. This involves such items as:

- managing the information security process and working on all the tasks relating to it,
- providing management with support when creating the policy for information security,

- coordinating the creation of the security concept, the contingency planning concept, and other sub-concepts and system security policies as well as issuing additional policies 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,
- coordinating projects relating to security,
- examining security issues, and
- initiating and coordinating controlling awareness-raising and training measures on information security.

Furthermore, the ISO is to be involved in all larger projects that could have a significant impact on information processing to ensure consideration of security aspects during the various project phases. Thus, the ISO should be involved both in planning and introducing new applications and IT systems and in case of new ICS components or significant changes to the infrastructure.

Requirements

For fulfilling such tasks it is desired that the Information Security Officer has knowledge and experience in the fields of information security and IT. Moreover, the Information Security Officer should have knowledge on the business processes of the organisation. As this task requires a variety of skills, the person appointed to this position should possess the following qualifications:

- Identification with the objectives of information security, overview of the tasks and goals of the organisation.
- Ability to co-operate and work in a team, also ability to assert oneself (almost no other task requires such skills and abilities in dealing with other people: The management level must be integrated again and again into a number of the main phases of the security process. Decisions must be requested and the staff must be included into the security process, possibly with help from the area's security officer.)
- Project management experience, ideally in system analysis and understanding of risk analysis methods.
- Basic knowledge on the processes and specialised tasks within the organisation are required; basic knowledge in the fields of IT and ICS.
- An Information Security Officer must also be willing to understand new areas and follow IT development . This role requires additional training so that the post-holder can perform the tasks required.

Co-operation and communication

Working with the employees and external personnel requires a high degree of skill since these people must be convinced of the necessity of the security safeguards, which some may perceive as a burden. Questioning of the employees regarding security-critical incidents and vulnerabilities represents another very sensitive topic. In order to guarantee success here, the employees must be convinced that honest answers will not cause them problems.

It is not only when talking to employees that Information Security Officers require excellent communication skills. It is equally important that the ISO is able to represent his/her opinion to the management of the public agency or company. He/she must therefore be self-confident and able to communicate so that he/she can, if necessary, object to a decision that is not compatible with the security objectives.

The Information Security Officer must be able to employ his/her ability to communicate so that there will be no misunderstandings in other specialised areas. For this it is particularly important to understand and respect the corresponding other linguistic worlds and cultures. For example, contact persons in the field of industrial control use other terms for IT equipment than IT experts.

Independence

It is recommended to install the position of the Information Security Officer as a staff department, i.e. a position directly allocated to the management level, which does not receive orders from other bodies. In any case the ISO must have the direct right of recitation at any time with the management of the public agency and/or company to be able to inform them on security incidents, risks, and safeguards. However, the ISO must also be informed comprehensively and early on what happened within the organisation as far as this is related to his/her activity.

Within the organisation the Information Security Officer should not be allocated to the IT department. Experience shows that this frequently results in that the tasks of information security is reduced to IT safeguarding and the holistic protection of information is moved to the background. This may result in that information are protected appropriately as long as they are exclusively processed on IT systems, but for example are left at the printer without protection after printing. The inherent conflict of tasks is another problem. It is, for example, problematic if an "active" administrator undertakes the role of the Information Security Officer in addition to his/her normal tasks, because there is a high probability of a conflict of interests. Since the roles are undertaken by one and the same person, as the Information Security Officer he or she may have to object to decisions that would facilitate his or her work substantially as administrators or for which their superiors have given strong approval (see also Section 4.10 *Interaction with other organisational units and management disciplines*).

Simultaneous performance of role together with data protection officer

A frequent question is whether the position of the Information Security Officer can be simultaneously performed by the data protection officer (regarding his/her tasks, 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, direct reporting paths to the management level should be available on all sides. There should also be consideration as to whether conflicting issues should also be notified to the auditing department.
- The Information Security Officer must have adequate resources to undertake both roles. If necessary the post-holder must be supported by appropriate personnel.

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

4.5 The IS Management Team

The IS Management Team supports the Information Security Officer by coordinating comprehensive safeguards in the entire organisation, by collecting information, and by performing control tasks. The precise form of the team will depend on the size of the organisation concerned, the desired level of security and the available resources. In extreme cases, the IS Management Team only consists of two persons – the Information Security Officer, who is responsible for all tasks within the security process in such case, and his/her deputy.

The tasks of the IS Management Team are in particular:

- specifying information security objectives and strategies and developing the information security policy,
- reviewing implementation of the security policy,
- initiating, directing and monitoring the security process,
- helping to draw up the security concept,

- examining whether the security safeguards planned in the security policy operate as intended, are appropriate and effective,
- designing training and awareness raising programmes for information security, and
- providing advice to specialists responsible, IT operations, area ISOs, possibly to ICS-ISO and management level, on questions regarding information security.

Composition of the team

In order to be able to perform their tasks effectively, the IS Management Team members should have knowledge of information security, technical knowledge of the IT, ICS and IoT systems used within the organisation and experience in organisation and administration. Furthermore, the IS Management Team should know the various fields of tasks and business processes of an organisation. In larger organisations it will be reasonable if the various specialised fields of an organisation have a representative in the IS Management Team, respectively. Such person undertakes representation in the IS Management Team in addition to his/her specialised tasks, contributes expertise and thus becomes a contact person for security questions of employees from this field.

4.6 Area and Project Security Officers and/or IT Security Officer

In large organisations it may be necessary to employ separate Security Officers in each of the various business areas.

Area Security Officer

The Area Security Officer is responsible for all the security issues relating to business processes, applications and IT systems in his/her area (e.g. department or remote office). Depending on the size of the business unit, the task of Area Security Officer can be assumed by somebody who is already entrusted with similar tasks, e.g. the person might already perform the role of Divisional Officer (if such a position exists). Care should be taken during selection of Area Security Officers to ensure that they are familiar with the tasks, conditions and work processes in his/her relevant business area.

IT Security Officer

In large organisations there can also be an IT Security Officer, who is responsible for security of IT. The ISO designs the information security management and creates the general security objectives and provisions; an IT Security Officer ensures that these are implemented technically. An IT Security Officer usually operates in the field of IT, whilst the ISO directly reports to the management level.

Project Security Officer

In case of large projects a Project Security Officer should be appointed to both clarify the security needs within the project and to enable secure inclusion of the project results into the business processes of the organisation. The Project Security Officer can be a member of the project or a member of the IS Management Team. The responsibility for information security always rests with the project manager and/or the management level. The ISO and/or the Project Security Officer supports the project management in case of questions regarding information security. Correspondingly, also the project management must budget and provide the required resources for information security.

The various business processes, applications and IT systems in an organisation frequently have different security requirements, which may be summarised into specific security policies and require different security safeguards. The analogous situation applies to the Project Security Officer, with the distinction that her/his role is project-specific instead of IT system-specific.

The tasks of the Project, IT and/or Area Security Officers include:

- implementing the procedures defined by the ISO,
- implementing the security safeguards in accordance with the IT system security policy or other specific security policies,

- collecting project-specific or IT system-specific information and forwarding it to the ISO,
- acting as contact person for the local employees,
- being involved in the selection of security safeguards used to implement the specific security policies,
- providing information on the training and awareness needs of employees,
- monitoring and evaluating log files at regular intervals, and
- notifying the ISO of any security-related problems.

Persons in these roles should possess the following qualifications:

- in-depth IT knowledge, as this makes it easier to talk to employees on-site and facilitates the search for security safeguards for special IT systems, and
- knowledge of project management – this is helpful when it comes to interviewing users and drawing up plans for the implementation and monitoring of security safeguards.

4.7 The ICS Information Security Officer (ICS-ISO)

Due to legal and organisations measures, organisations with industrial control components (ICS) should appoint an officer for implementation of information security requirements in this area.

Industrial control systems include numerous security requirements that differ significantly from the requirements of general office IT. In the ICS area, IT systems and applications frequently are used for a very long period. Often, the life cycle of such objects is more than 10 years.

However, applications and IT systems from the field of office IT are used increasingly within ICS areas. These are used as per their intended use for periods that are longer than usual periods in office environments.

The organisation should appoint an ICS Information Security Officer (ICS-ISO) to meet the special requirements in the field of industrial control and to include the security organisation from the field of industrial control in the overall ISMS. The ICS-ISO should be a member of the IS Management Team. Furthermore, the ICS-ISO should be present in the IS Coordination Committee (see Section 4.8 *IS Coordination Committee*). Indeed, the issue of industrial control does not affect all areas, but synergies can be used for the producing areas due to possible changes of office IT.

Depending on the size of the organisation it can be reasonable to distribute the tasks for the overall ISMS and the ISMS in the ICS area to different personnel resources.

The security organisation of industrial control should be included into and operated in the security organisation of the whole organisation. There must be close cooperation between the ICS-ISO and the ISO to use synergies and avoid bad planning as well as risks. Particularly the employees of building services and the IT experts are further contact persons within the organisation.

The structures that are suitable for a security organisation in the field of ICS highly depend on the present structures and the attuned processes within an organisation. Basically, communication between all parties involved must be ensured. All parties must have a basic understanding of the corresponding particularities of the other area. Only previous understanding of culture and terminology of the corresponding areas may avoid misunderstandings.

The tasks of the ICS Information Security Officer are as follows:

- implementing the generally applicable security provisions of the information security policy and further policies in the field of ICS,
- pursuing joint objectives from the field of industrial control and overall ISMS and actively supporting projects,

- performing risk analysis for the ICS area meeting the provisions of risk management,
- creating and providing training on security policies and concepts for the ICS area involving the requirements from safety and security,
- closely cooperating with the Information Security Officer,
- serving as a contact person regarding ICS security for local employees and within the whole organisation,
- creating ICS security safeguards and participating in implementation,
- creating required documents on ICS security and communicating these,
- determining information on training and awareness needs of employees in the ICS area and initiating activities, and
- processing security incidents in the ICS area together with the Information Security Officer.

The ICS-ISO should have the following qualifications:

- special knowledge regarding the processes within the organisation and the industrial control,
- sufficient IT knowledge to be able to comprehensively answer questions of local employees, IT experts and further parties,
- knowledge on threats and vulnerabilities within the industrial control,
- knowledge on risks for office IT used within the ICS area,
- knowledge on project management, and
- knowledge on the topics of change management and business continuity management.

4.8 IS Coordination Committee

The IS Coordination Committee is not usually a permanent committee in an organisation, rather it is called into being as required (e.g. for planning larger projects). Its task is to coordinate the interaction among the IS Management Team, the specialists responsible, the Security Officer and the management of the public agency and/or company.

Like with the IS Coordination Committee, there is an IT Coordination Committee in many organisations. However, this is no continuous body. Its task is to coordinate the interaction between the representatives of the IT users, the ISO and the management of the public agency and/or company.

It is a good idea to have the two coordination committees cooperate as far as possible and to also staff them as identical as possible.

Composition of the IS Coordination Committee

The IS Coordination Committee should reflect the various fields of tasks of an organisation. The IS Coordination Committee should include at least the following roles: a person responsible for IT, the Information Security Officer and representatives of the user. As frequently personal data also are affected, the Data Protection Officer also should be a member of the IS Coordination Committee. If the organisation has an ICS Information Security Officer, he/she should also be represented in the IS Coordination Committee. If a similar body already exists in the organisation, its tasks could be extended accordingly. However, it is advisable to install an IS Coordination Committee and to regularly convene to underline the importance of information security.

4.9 The Data Protection Officer

Data protection is often treated with lower priority as it supposedly impairs efficient information processing although it is based on legal regulations in Germany and many other countries and infringement of the corresponding right to informational self-determination may result in high fines and terms of imprisonment.

Often, the tasks of the Data Protection Officer are transferred to persons having another role that may result in a conflict of interests with the new function, e.g. by performing self-control in their original function (e.g. head of IT).

To avoid this, a competent and qualified contact person for data protection issues should be appointed, who accompanies any aspects of data protection within the organisation and ensures appropriate implementation and sufficient control. In such function, he/she closely cooperates with the Information Security Officer, is part of the IS Coordination Committee, is independent from instructions, and directly reports to the management of the public agency and/or company.

If implemented appropriately, data protection will promote work flows rather than making them more difficult. If a government agency and/or a company collects too many personal data, deletes personal data too late, or transmits personal data without authorisation, it not only violates the data protection law, but also causes an increased administrative workload and additional costs. Data protection is above all an important element of citizen- and customer-friendly behaviour, because it makes the procedures transparent.

Every organisation should appoint a Data Protection Officer. In many areas the appointment of a Data Protection Officer even is required by law. Compliance with the data protection requirements also must be ensured in organisations not having appointed a Data Protection Officer. This may also be performed by the IS Management Team or by internal auditing.

Requirements profile

Only persons disposing of the specialised knowledge and reliability required for fulfilling the tasks can be appointed as Data Protection Officer. Fulfilling the task requires technical, organisational, and legal know-how. The German regulatory data protection authorities recommend use of the Standard Data Protection Model [SDM] for efficient and complete fulfilment of tasks. The Data Protection Officer should know and be able to securely use the corresponding legal regulations, area-specific data protection regulations and the special regulations applicable for the organisation. Above all, the Federal Data Protection Act and the EU General Data Protection Regulation are important legal standards for data protection in Germany. The Data Protection Officer should furthermore have good knowledge of the organisation and profound knowledge in the field of information technology. If he/she lacks the technical qualification in sub-areas, he/she must be provided with the opportunity to gain corresponding further qualification. The Data Protection Officer should be very familiar with the tasks and modus operandi of his/her government agency and/or company, based on his/her own experiences, if possible, in order to be able to fulfil his/her control and counselling tasks.

The Data Protection Officer does not have to be commissioned exclusively with such functions. Depending on the type and extent of the personal data processing and the related data protection problems, it may make sense to assign more tasks to him/her additionally. This will be applicable above all in case of smaller organisations. Special care must be taken to ensure that no conflicts of interest or dependencies are created that could endanger his/her ability to perform the required tasks. It is also possible to combine the functions of the Data Protection Officer and the functions of the Information Security Officer; regarding the framework conditions, see also Section 4.4 *The Information Security Officer*.

Obligation of involvement

The Data Protection Officer must have the direct right of recitation at any time with the management and must be informed about the events in the government agency and/or company in a comprehensive and timely manner, insofar as these refer to his/her work. He/she must be involved in data protection-relevant processes and plans referring to handling personal data must be disclosed to him/her. If needed, he/she must be supported by other employees with further legal or technical knowledge.

Responsibilities and tasks

The Data Protection Officer must contribute that his/her organisation takes into account the requirements of data protection in a comprehensive manner. He/she must check the compliance with the data protection provisions in all areas. He/she performs his/her tasks mainly be counselling and

inspections. His/her primary task is to provide advice. For the employees, the Data Protection Officer should be contact person regarding all questions in terms of data protection they can confidently turn to at any time. In the event of vulnerabilities and omissions, he/she should initially seek constructive solutions together with the persons involved.

The Data Protection Officer supports the management of the public agency and/or company in assuming their responsibility for maintaining the protection of personality rights and in avoiding incidents detrimental to the reputation of the organisation. He/she should also establish and maintain contact with the Personnel and/or Supervisory Board. A good collaboration is not only desirable because of the sensitivity of personnel data processing.

In the individual case, the specific customisation of the Data Protection Officer's tasks depends on the tasks to be performed, but also on the size, the design, and the structure of the relevant government agency and/or company.

4.10 Interaction with other organisational units and management disciplines

In addition to the information security management, most organisations also have other areas performing tasks in the field of information security or having comparable tasks so that it will be reasonable to agree on a coordinated procedure and on interfaces. Often such areas are organised as separate disciplines and partially also in other organisational units. These areas have in common that they all, from different points of view, have the objective of protecting the values of the organisation. Thus, many of these areas have “protection” as part of their name. In addition to information security management, this includes the subjects of data protection, protection of objects, protection of persons, protection of classified information, business continuity management or risk management. Correspondingly, there may not only be a Data Protection Officer in addition to the Information Security Officer, but there also may be an officer for protection of classified information, a business continuity officer or an auditor. In organisations with a production area, also the cooperation with the persons responsible for security of products and plants is important.

Collaboration with the IT operations

Many subtasks of security management directly depend on tasks of IT operations. The ISO creates specifications for secure operation of IT systems and networks, and the IT operations must implement these specifications. Thus, security management and IT operations must closely collaborate and regularly coordinate on procedures as well as on current risks and security requirements newly to be implemented. Correspondingly, in larger organisations it may be reasonable to appoint an IT Security Officer as a contact person of the ISO in IT operations. Frequently, such person is named IT Security Officer, IT Security Manager or also IT Security Coordinator.

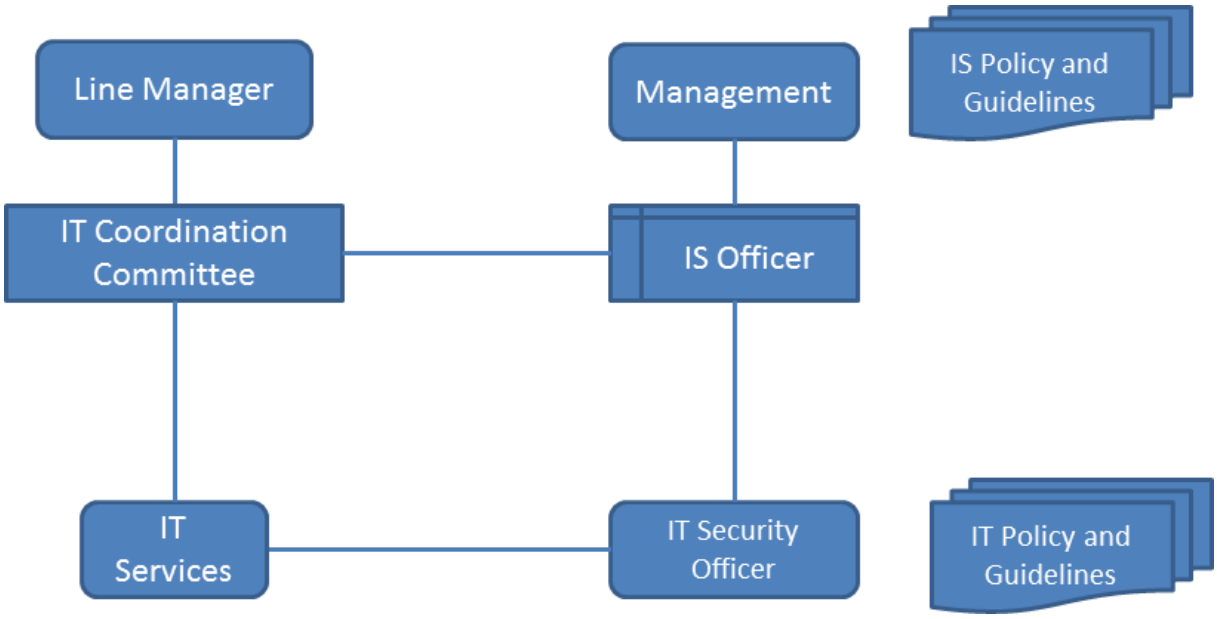


Figure 7: IS organisation and IT operations

Avoid role conflicts

When designing the roles and distributing the tasks, the tasks that can be performed simultaneously and the possible sites of role conflicts should be taken into account. From the view of the information security management, it should be clarified to what an extent the ISO may adopt further roles such as the role of the business continuity officer.

Basically, such roles do not exclude each other. However, factors such as size and orientation of the organisation, IT penetration of the business processes and characteristics of security management are decisive.

Fundamentally, the following aspects should be clarified in advance when taking over further tasks:

- The interfaces between the various roles should be clearly defined and documented.
- If topics with potential of conflict occur, an entity able to clarify this should be named, e.g. internal auditing.
- It must be ensured that persons assuming more than one role are adequately qualified and are provided with enough resources to perform their tasks.

However, there are also roles that cannot be combined with the tasks of information security management without further ado. This may include e.g. roles such as reviser or auditor, but this also depends on the concrete environment of the tasks. Basically, in case of a controlling activity there is always the problem that the controlling persons should not check anything designed by themselves.

4.11 Involvement of external security professionals

In some cases it might be necessary to employ external security professionals as part of the internal security organisation. If crucial roles like the ISO cannot be filled by own staff, the role must be assigned to qualified external staff. The required qualifications are described in the previous sections of this chapter.

Especially in small companies or public authorities, there can be circumstances where it is necessary to rely on services of an external ISO instead of establishing a suitable position in-house.

From experience, in-house security experts often do not have enough time to pay attention to and analyse all determining factors (e.g. legal requirements or technical aspects) necessary to fulfill the role of an ISO. Sometimes they are also missing essential requirements. In such cases it is also

reasonable to rely on external experts. This must be documented, so the management can provide the required resources.

Action points on 4 Organisation of the security process

- Stipulate roles for designing the information security process
- Assign tasks and areas of responsibilities to the roles
- Stipulate the human resources required for the roles
- Document IS organisation
- Integrate information security management into the generic processes
- Take into account the involvement of external experts

5 Documentation within the security process

A multitude of different documents and descriptions is created before and during the security process. In this respect, it should always be ensured that the time involved in the preparation of documentations remains within reasonable limits. The documentation of the security process should be expressive so that the decisions and implementations made at a former point in time will be understandable later on.

This section describes ideal and typical requirements and methods for documentation of the security process. The documentation process can and should be adapted depending on the selected IT-Grundschutz approach and the present framework conditions. In particular for the Basic Protection, the documentation process should be kept as simple and practical as possible.

If later certification of ISMS is desired, creation of certain documents will be mandatory (see Section 11 *Certification according to ISO 27001 on the basis of IT-Grundschutz*). Besides, documentation efforts should be minimised as much as possible. If IT-Grundschutz states that something must be documented, it will not be required to create independent documents for this in most cases. Generally, it will be sufficient to take down the required information at a suitable location, e.g. in a Wiki, in present texts or tables.

5.1 Classification of information

Appropriate protection of information requires that importance of such information for the organisation is clear. A classification scheme describing the levels of significance and the delimitation of the individual levels is required to be able to easily communicate on the value of information within an organisation and also with other organisations.

Thus, a reasonable approach will be to elaborate a classification scheme that enables all employees to derive from such scheme the correct classification for any type of information without requiring explicit identification of the same. The classification scheme should not be too complicated so that it is easily understandable and usable.

It is reasonable to use the basic values of information security as a basis and to classify information with regard to their confidentiality, integrity and availability. Depending on the organisation, also further or other parameters can be used, e.g. if such parameters have been used already in other contexts within the organisation. However, one disadvantage of extending the classification scheme is that the classification becomes more complex. This makes it more difficult for the employees to understand delimitation of the individual levels and to use the scheme. Another disadvantage is that it is more complex to create joint understanding of the classification of information with other organisations.

Classification of confidentiality often uses the levels *public*, *internal*, *confidential* and *strictly confidential*. Regarding availability, classification can be made e.g. with regard to the expected and/or tolerable time until restoration in case of a failure, such as *one hour*, *one day*, *one week*, *one month*. Classification of integrity is harder; a possible classification includes *essential*, *important* and *normal*. Criteria for this might be the possible effects in case of loss of integrity as well as their severity, or the efforts made for ensuring integrity.

In simple cases, such as in the context of Basic Protection, a two-level classification can be sufficient already in the beginning, e.g. by only differentiating between internal ("everything in the Intranet") and public information. In such case it is recommended to classify the information intended for publication as such ("public"), but only such information.

This classification is an essential prerequisite for selection and use of adequate security safeguards later on.

Identification: It is desirable to identify all information already at the time of generation of the same to be able to protect them appropriately and consistently during their whole life cycle. However, experience shows that this is difficult. This is because a classification scheme is easy to create, but

hard to maintain during ongoing operation so that all employees make use of it in a consistent and uniform manner. Furthermore, it should be considered that the classification may change during the life cycle of the information.

A positive side effect of the classification of data is that this shows the data that are unnecessary or outdated and/or that are not used any more. Consistent classification aids in reducing waste data.

Creation and operation of a functional process for classification of information should include establishing appropriate roles for this and specification of the tasks of such roles.

The following table shows a comprehensive example for possible roles to make clear required tasks. Here, suitable adjustments can be made in practice. There always should be at least one role of a person responsible for the classification process as well as the roles of such persons that comply with and/or implement this process.

Role	**German role name**	**Who can take over the role?**	**Tasks**
Data Creator	Ersteller	every employee	• creates data • first classification
Data Owner	Fachverantwort-licher	specialist responsible/line superior	• specifies regulations on classification within his/her area • clarifies classification questions with creators • monitors classification process on the side of the creator
Data User	Benutzer	every employee	• uses data • complies with rules on classification • provides feedback on classification levels
Data Auditor	Klassifikations-Verantwortlicher	Compliance Manager	• creates organisation-wide classification strategy and specifications • provides aids and explanations • clarifies classification questions with specialists responsible and users • monitors classification process on the side of the specialist responsible • coordinates with: risk management, ISO, Data Protection Officer

Table: Tasks and processes for classification of data

A typical example for a classification scheme refers to the German classification for protection of classified information:

- VS-NUR FÜR DEN DIENSTGEBRAUCH (CLASSIFIED - FOR OFFICIAL USE ONLY)
- VS-VERTRAULICH (CLASSIFIED - CONFIDENTIAL)
- GEHEIM (SECRET)

- STRENG GEHEIM (TOP SECRET)

However, such scheme is focused on the small area of classified material (VS), i.e. on the information or objects requiring confidentiality for the public benefit. This includes large gaps regarding the multitude of information that typically arise within a company or a public agency, which also require protection. Thus, in organisations where classified material only represents a minor share of the processed data, it is reasonable having an own classification scheme for the large part of business-relevant and partially business-critical information.

Action points on 5.1 Classification of information

- Create a classification scheme enabling correct, uncomplicated and understandable classification of information

5.2 Information flow within the information security process

In the various steps of the information security process a multitude of various reports, concepts, policies, notifications on security-relevant events and further documents on information security of the organisation are created. The documents must be meaningful and understandable for the corresponding target group. As not all of such information are suitable for the management level, the task of the ISO is to collect and process such information and to correspondingly edit them in a brief and clear manner.

This section comprehensively describes the essential aspects regarding appropriate documentation as well as appropriate information flow. Consideration of such aspects will be beneficial for creation of a good documentation. They are proven and recommendable and must be adapted to the circumstances of the organisation. This particularly applies in the context of Basic Protection. They will become mandatory within the scope of certification; in any other context they should be considered to be best practice.

5.2.1 Reports to management level

In order for the management of the company and/or public agency 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 providing this data and covering the following aspects, among others:

- Status and implementation level of the security concept
- Results of audits and data protection checks (see also General Data Protection Regulation [DSGVO])
- Reports on security incidents
- Reports on previous successes and problems in the information security process
- Reports on the reduction of existing implementation deficits and the correspondingly connected risks (risk handling plan, see BSI-Standard 200-3)

The management level must be informed regularly and in an appropriate form of the results of the examinations and the status of the security process by the ISO. This should include pointing out successes, problems and potential improvements. The management level is aware of the management reports and organises any measures that are required.

Moreover, the Security Officer elaborates the security concept and ensures its implementation and regular updating. The security concept is approved by the management level.

5.2.2 Documentation within the information security process

For many reasons, the documentation of the IS process on every level is key to its success. Only if the decisions are adequately documented,

- decisions will become comprehensible,
- processes will become repeatable and standardisable,
- weaknesses and failures can be identified and avoided in the future.

Depending on the subject and purpose of a document, the following different types of documentation can be differentiated:

- Documents for security management (target group: security management)

Concepts, policies, reports and further documents are created within the scope of the activities of the information security management. The decisions made can only be understood later, actions can only be repeated, and weaknesses can only be detected and avoided in the future when the decisions are adequately documented.

The quantity and the characteristics of the documentation depend on the requirements of the corresponding organisation and can be very different. Examples of the documents to be created include the following:

  - Security concept with reports on risk analysis,
  - Training and awareness-raising concept,
  - Audit or revision reports.

- Technical documentation and documentation for work processes (target group: experts)

  Here, the current state of business processes and the correspondingly connected IT systems and applications is described. Often, the level of detail of technical documentations is an issue of dispute. A more practical approach is that other persons with comparable expertise in such area must be able to understand the documentation and that the administrator must rely on his/her knowledge, but not on his/her memory to restore the systems and applications. In case of security drills and when handling security issues the quality of the present documentations should be assessed and the gained knowledge should be used for improvement. Such type of documentations includes, but is not limited to:

    - Installation and configuration manuals,
    - Instructions for recovery after a security incident,
    - Documentation for testing and authorisation procedures,
    - Instructions on how to respond to malfunctions and security incidents.

- Instructions for employees (target group: employees)

  The information security policy is the document containing the basic statements on handling of information security in the organisation.

  In addition, the security safeguards to be implemented must be documents by means of policies in a manner that is understandable for the employees. The employees must be informed on and correspondingly trained with regard to the existence and importance of such policies. This group of documentations include, for example:

    - work processes and organisational rules,
    - policies for using the Internet,
    - response to security incidents.

- Recording of management decisions (target group: management level)

  Basic decisions on the information security process and on the security strategy must be recorded so that they are understandable and repeatable at any time.

- Laws and regulations (target group: management level)

  A multitude of laws, regulations and instructions can be relevant for information processing. The laws, regulations and instructions imposing particular requirements on business processes, IT operations and information security in the present case and the concrete consequences resulting from this should be documented.

- Reference documents for certification (target group: organisations with the objective of certification)

  If an organisation desires certification, then various documents must be created and updated for auditing. These documents are handed over to the auditors and to the certification body at BSI, are assessed, and then the decision in favour or against certification is made on such basis. The documents required for certification are maintained on the Internet in the list of reference documents. This includes, for example, policies for risk analysis, for control of documents and records, for auditing the management system for information security, and for control of corrective and preventive measures.

- Documentation in the ICS area (target group: users)

  Many of the documents on information security from the field of IT area can be taken over to the field of industrial control. However, some of the documents from the field of IT cannot be transferred to the field of industrial control without further ado. Here, documents for the field of ICS must be newly created, modified or changed according to the requirements. Frequently, it is reasonable to create a derived policy for information security and own policies and work instructions for the field of industrial control. It is to be considered that all derived documents should be integrated into the ISMS of the organisation.

It must be ensured that all documentations are kept up-to-date. For this, the documentation must be involved in the change process.

5.2.3 Requirements on the documentation

An appropriate documentation of the information security process should meet a number of requirements regarding labelling, level of detail, updating, medium, security, and data protection. These are described in detail in the following.

Minimum requirement for the labelling of documents used for security management

The documents created, edited, and administered in the context of security management must be informative and understandable for the particular target group. A uniform document format should be used, if possible. This improves their understandability and their handling. The documents must be labelled so that they can be found and identified quickly when needed. For this reason, the following specifications must be present at a minimum:

- Unique label (informative title),
- Creator / author / document owner,
- Function of the author,
- Version number,
- Date of last revision, date of next planned revision,
- Release on / by,
- Classification (confidential contents must be classified and labelled as such, and the documents must be stored securely), and
- Authorised roles (distribution list).

The following information can also be provided as an option:

- Source information,

- Retention period, and
- Overview of changes.

External documents relevant for security management must also be labelled and administered appropriately.

Level of detail

The following principle applies in terms of the level of detail in the individual documents: “According to the goal and purpose of the document”. Strategy documents such as policies should be brief and concise, but should still be informative. The documents created during the conception phase should contain detailed information so that the decisions made based on this information can be understood later on. All decisions as well as the information on which the decisions are based must be documented.

The policies and instructions for employees must be especially clear and easy to understand. Simple check-lists are often adequate for certain areas. Check-lists provide a quick overview, help ensure that nothing is forgotten, and ensure that the individual steps are followed in the correct order.

Change management

All documents on change management should be updated regularly. For this, it is recommended to apply a change management procedure to record, assess, approve and understand all changes. Clear change management instructions must be specified in writing for all documents for this purpose. The procedure should also specify how users can submit suggestions for change, how these suggestions are then evaluated and, if necessary, how to implement them. The change management process for security management is to be integrated into the overall change management process of the organisation.

Update intervals should be specified for each document. Annual checks have been found to be appropriate for most of the documents.

The mechanisms triggering the change management process are to be integrated into the corresponding processes (e.g. personnel administration, building management, inventories). The Security Officer acts as a controlling body. The owner of a particular document is responsible for updating the document and submitting change requests for the document.

Documentation medium

Documents for security management do not always need to be available on paper. Local or Internet-based software tools can also be used for documentation. They are able to store all information necessary and can be used at different locations as well as in a collaborative manner.

The documentation medium should be selected depending on the needs, phase (planning, implementation or auditing) or subtask. Even the persons for whom the documents are intended and how familiar they are with the various media should be taken into account. For example, one person may prefer paper documents while another person may find it essential to be able to search for or filter information from electronic documents.

Security and data protection

Since the documents for security management contain sensitive data on the organisation as well as personal data, information security and data protection must be guaranteed. The integrity, and especially the confidentiality of the documents must be guaranteed in addition to their availability. The various documents for emergency management should be classified according to their confidentiality, labelled accordingly, and protected by suitable safeguards.

The authorised recipients of each document should be named in the document. Access to the documents is to be limited to those persons who need the information they contain to perform their tasks (“need to know” principle). It is therefore recommended to modularise the documents accordingly. This allows the right information to be distributed to the right recipients. An overview containing the number of the classified documents, their types (e.g. paper or DVD), to whom they are

distributed, as well as information on correct and complete updates, their destruction, or their return should be available in the organisation.

5.2.4 Information flow and reporting routes

All parties involved must be informed promptly on the various activities within the scope of the security management. However, it is not reasonable to arbitrarily spread detailed information on the security process. Thus, it must be clarified who will communicate which details of the security process when and using which internal and external bodies. Furthermore, it must be specified which communication channels are used for the respective contact persons, and how these channels are protected.

Prompt updating for reporting routes and the specifications for the information flow 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.

Basic specifications on information flow and on the reporting routes regarding the information security process should be documented in a corresponding policy and should be passed by the management level. The *Guideline on information flow and on the reporting routes* should regulate particularly the information flows critical for the information security process. Here, differentiation is to be made between obligation to provide and obligation to obtain.

Using synergy effects for the information flow

Many organisations have already defined processes to provide services or IT operations. Frequently, synergy effects can be used and aspects of information security can be included in already existing processes. For example, reporting routes for IT security incidents could be integrated into IT operations or capacity planning could be expanded to include aspects of contingency planning.

Much of the information that is gathered for security reasons can also be used for other processes. security safeguards also have other positive subsidiary effects and optimising processes has paid off in particular. For example, the appointment of information owners or grading information by homogeneous assessment criteria are often relevant for many departments of an organisation. A summary of the dependence of business processes on IT and/or ICS systems and applications is also appropriate for other issues apart from security management. For example, often this facilitates the precise assignment of IT costs to specific business processes or products; these are frequently assigned to overheads.

Action points on 5.2 Information flow within the information security process

- Document basic specifications on information flow and on the reporting routes regarding the information security process in a corresponding policy and present them to the management level for passing.
- Inform management level of the results of checks and the status of the information security process
- If required, obtain decisions on the necessary corrective measures
- Document all sub-aspects of the whole information security process clearly and keep the documentation up to date
- As required, assess the quality of the documentation and, if necessary, improve or update it
- Keep reporting routes that relate to the information security process up to date
- Find synergies between the information security process and other management processes

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

Drawing up of the security concept for the organisation will be made in accordance with the Basic Protection approach, if the following prerequisites are met:

- an information security process has been initiated,
- the security policy and information security organisation have been defined,
- a summary of the present assets of the organisation has been created,
- the Basic Protection has been selected as IT-Grundschutz approach.

For the security concept, organisational, infrastructural and technical requirements from the IT-Grundschutz Compendium should be met for the components of business processes, applications and IT systems. These are classified in modules so that they can build on each other.

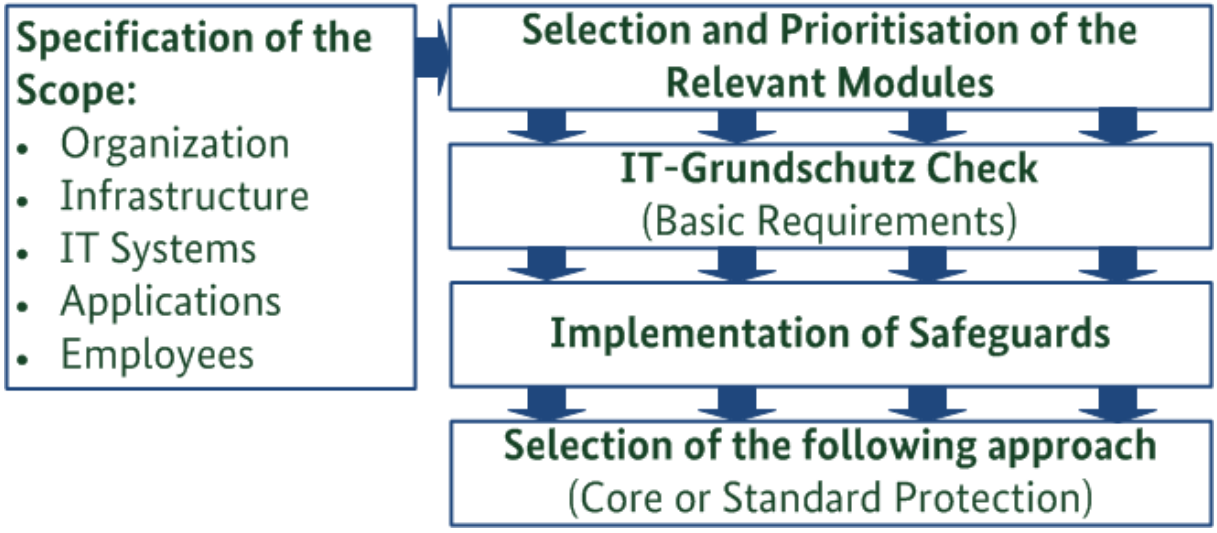


Figure 8: Basic Protection

Drawing up of a security concept according to the Basic Protection is structured with the following fields of action which are presented in more detail below:

- Specification of the scope:
  The information domain for which the security concept should be drawn up and implemented must be defined.
- Selection and prioritisation:
  The considered information domain must be reproduced using the present modules from the IT-Grundschutz Compendium.
- IT-Grundschutz Check:
  This step is to check whether the basic requirements according to IT-Grundschutz have been implemented already in parts or completely, and which security safeguards are still missing.
- Implementation:
  Suitable security safeguards must be specified and implemented for the basic requirements not met so far.
- Selection of the following approach:
  The Basic Protection is intended as an initial approach. Thus, the time and the type of IT-Grundschutz approach for raising the security level must be specified.

Contrary to Standard Protection, the fields of action in case of Basic Protection do not represent a closed cycle, but an entry approach that can be continued with the Standard Protection (possibly with Core Protection as an intermediate step).

6.1 Specification of the scope for Basic Protection

When drawing up of a security concept, the area of the organisation to be covered (scope) must be specified first.

The scope may include the whole organisation or just individual areas. In any case, the scope should be clearly delimited and should be reasonably self-contained, with a few, uniquely defined interfaces. Thus, at first an organisation could implement the Basic Protection for a newly added department with its business processes and assets, for example. Detailed information of delimitation of the scope are included in Section 3.4.3 *Specification of the scope and the content of the security policy*.

Information domain

The scope for drawing up of the security concept will be referred to as “information domain” in the following. An information domain comprises all the infrastructural, organisational, personnel and technical components which serve to perform tasks in a particular field of information processing. An information domain may comprise to the entire information processing of an organisation or to individual areas defined by organisational or technical structures (e.g. department network) or joint business processes and/or shared applications (e.g. HR information domain). The relevant components of the considered information domain are identified for drawing up of the security concept on the basis of the first acquisition performed already during the preliminary work (see Section 3.2.4 *First acquisition of processes, applications and IT systems*).

6.2 Selection and prioritisation for Basic Protection

The next step is to reproduce the considered information domain by using the processes, applications, IT systems, communication links and rooms identified at first acquisition and the present modules from the IT-Grundschutz Compendium. This results in an IT-Grundschutz model of the information domain that consists of the various modules, possibly used several times, and contains the security-relevant aspects of the information domain due to use of the modules.

6.2.1 Modelling according to IT-Grundschutz

The corresponding modules of the IT-Grundschutz Compendium must be selected and implemented to model a generally complex information domain according to IT-Grundschutz. In the IT-Grundschutz Compendium the modules are separated into process-oriented and system-oriented modules to facilitate selection. A summary of the structure of the IT-Grundschutz Compendium including the system and process modules is included in Section 8.3.1 *The IT-Grundschutz Compendium*.

IT-Grundschutz modelling entails determining whether and how the modules of a given layer can be used to map the information domain. Depending on the considered module, the target objects of such mapping can be of different types: individual business processes or components, groups of components, buildings, properties, organisational units, etc. If individual target objects cannot be mapped directly using the present components, it must be ensured that similar, generalised modules are considered.

6.2.2 Order of module implementation

The essential security requirements must be fulfilled early and corresponding security safeguards must be implemented to cover basic risks and establish holistic information security. Thus, IT-Grundschutz proposes an order for the modules to be implemented.

In the IT-Grundschutz Compendium, the Section *Layer model and modelling* describes when it is appropriate to use an individual module and which target objects it should be applied to. Furthermore, the modules are labelled with regard to whether they should be implemented with higher or lower priority.

This label only shows the reasonable temporal order for implementation of the respective requirements of the modules and does not represent an weighting of the modules with regard to each other. Basically, all modules of the IT-Grundschutz Compendium relevant for the corresponding information domain must be implemented.

Labelling of the modules only is a recommendation for an order of the various modules to obtain reasonable implementation. Here, every organisation may specify another order that is reasonable for such organisation.

6.2.3 Assignment of modules

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

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

6.2.4 Determining concrete actions from requirement

Modelling has been used to select the modules of the IT-Grundschutz Compendium that are to be implemented for the individual target objects of the considered information domain. The modules state the requirements that are typically suited and appropriate for these components.

Now, for drawing up of a security concept or for an audit, the individual requirements must be processed and suitable security safeguards must be formulated for fulfilment; here, the implementation recommendations of many modules provide support. More detailed information on this can be found in Section 8.3.6 *Adapting module requirements*.

6.3 IT-Grundschutz Check for Basic Protection

The business-critical information and core processes of the organisation had been determined and the affected applications, IT systems, networks and rooms had been acquired during the preliminary work of first acquisition (see Section 3.2.4 *First acquisition of processes, applications and IT systems*) even before selecting an IT-Grundschutz approach. The considered information domain was reproduced using the present modules from the IT-Grundschutz Compendium. Now, selection and prioritisation of the IT-Grundschutz modules (as described in the previous section) are used as check plan to employ a gap analysis to determine the basic requirements that are fulfilled sufficiently or only insufficiently.

In case of the IT-Grundschutz Check to be employed here for Basic Protection, only the basic requirements must be fulfilled. In case of a standard or Core Protection, a separate IT-Grundschutz Check that also includes the standard requirements of the corresponding modules is to be performed within such approaches. The results of the IT-Grundschutz Check to be performed for Basic Protection should be edited so that they can be integrated directly into the standard or Core Protection to avoid additional efforts and obtain synergy effects.

The IT-Grundschutz Check consists of three different steps regardless of the IT-Grundschutz approach. The first step entails making the organisational preparations and in particular selecting the relevant contact people for the gap analysis. In the second step gap analysis is performed using interviews and random samples. In the final step, the results of gap analysis are documented, together with the rationale behind it.

Organisational preliminary work for the IT-Grundschutz Check

First, all internal papers regulating the security-relevant processes, should be inspected. These documents can be helpful when determining the level of implementation.

Suitable interview partners must be identified. A main contact person should be specified for each module used to model the IT system. The requirements in the modules include the roles that are responsible for implementation of the requirements. Based on this information, the appropriate contact persons for the relevant subject matter in the organisation can be identified. For example, in case of the modules of the APP *(applications)* layer these are the administrators of the individual applications.

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

A time schedule should be created for the upcoming interviews. Special attention should be given here to co-ordinating appointments with people from other organisational units or other agencies/companies. It is also appropriate to agree on alternative meeting dates.

Performing the gap analysis

When determining the achieved security status the security requirements of the respective module are processed progressively. These can be fulfilled completely, partially or not fulfilled. Thus, one of the following statements is possible as implementation status, respectively:

"unnecessary"	Fulfilment of the requirement in the proposed way is not necessary because the requirement is not relevant in the considered information domain (e.g. because services have not been activated).
"yes"	Appropriate safeguards have been implemented completely, efficiently and appropriately for the requirement.
"partially"	The requirement only has been implemented partially.
"no"	The requirement has not been fulfilled yet, i.e. suitable measures have not been implemented yet to a large extent.

It is useful to have the module texts as well as the implementation recommendations or other supplementary material at hand during the interviews. The purpose of the IT-Grundschutz Check should be briefly presented to the interviewed persons. Continue by naming the requirement names and briefly explaining the requirement. The communication partner should be given the possibility to respond to the requirements and safeguards implemented already, and then unsolved questions should be discussed.

At the end of each module, the result should be provided to the interviewed persons (implementation status of the requirements: unnecessary/yes/partially/no) and such decision should be explained.

Documentation of results

The results of the IT-Grundschutz Check should be documented such that all those involved can understand them, and they can be used as the basis for implementation planning for those requirements and measures where deficits still exist. Suitable aids providing support for drawing up and updating any documents required within the scope of the security process should be used, e.g. special IT-Grundschutz tools or own tables. The IT-Grundschutz web pages also provide supporting forms for the respective modules.

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

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

- Persons responsible: Which employees are responsible for complete implementation of a deficient requirement? Until when is it to be implemented?
- Remarks: Such field is important to be able to understand decision later on. In the case of requirements whose implementation appears unnecessary, the rationale for this should be stated. In the case of requirements that have not yet been implemented or only partially implemented, this field should document which measures still have to be implemented. Any other notes which will assist in rectifying deficits or which need to be considered in the context of the requirement should also be entered here.
- Deficits/estimation of costs: Regarding requirements not fulfilled or only partially fulfilled, the respectively connected risks should be determined and documented in a suitable manner. Furthermore, the financial and personnel efforts for removing the deficits should be estimated.

These steps are described in detail in the Section 8.4 *IT-Grundschutz Check*.

6.4 Implementation

This section describes how the security safeguards for Basic Protection are derived from the requirements, and how they can be planned, performed, supported, and monitored. The results of the IT-Grundschutz Check, i.e. of the gap analysis, are present.

In general, all identified basic requirements should be fulfilled for Basic Protection. There are usually only limited resources in terms of money and personnel available to fulfil the basic requirements. Thus, the objective of the steps described in the following is to achieve fulfilment of the intended basic requirements in a manner that is as efficient as possible; a detailed description for all IT-Grundschutz approaches is included in Section 9 *Implementation of the security concept*:

- Reviewing the results of the study:
  As a first step, the missing or only partially fulfilled basic requirements should be evaluated in an overall view.
- Consolidation of the basic requirements
  This step is to first consolidate the basic requirement to be fulfilled yet.
- Estimating the costs and expense
  The investment costs and the correspondingly required personnel should be documented for each basic requirement to be fulfilled.
- Determining the implementation order of the basic requirements:
  If the existing budget or staffing resources are not sufficient to be able to implement all the missing basic requirements immediately, the order in which these requirements will be implemented must be determined.
- Specification of the tasks and responsibilities
  The persons and the time for fulfilment of the basic requirements must be specified.
- Basic requirements accompanying the implementation
  It is particularly important to design basic requirements accompanying the implementation, e.g. training, in advance and to include them when planning the implementation.

6.5 Selection of a following approach

Information security must be lived. To enable the maintenance and continuous improvement of the security level, you not only need to implement and continuously update the required security safeguards, but also need to check the whole process of information security regularly in terms of its effectiveness and efficiency.

Basic Protection is an IT-Grundschutz approach for entry to be able to identify and implement the most important security recommendations for the selected field of use in a timely manner, respectively. Thus, the objective is to create a complete security concept in accordance with Standard

Protection on the medium term. The Core Protection could be added to the now created security concept as an intermediate step after Basic Protection and before Standard Protection.

After implementing Basic Protection, it should be decided promptly when to start with the required process of improvement. Depending of the security requirements and the available resources it should be decided whether the next step should include drawing up of a security concept according to the Standard Protection or the Core Protection. Information on selection are included in Section 3.3 *Decision on approach*.

7 Drawing up of a security concept according to the Core Protection approach

IT-Grundschutz of BSI provides a holistic protection of all business-relevant information of an organisation. In case of organisation still having high need for action in the field of information security it can be reasonable to limit themselves to safeguarding of the essential assets in the beginning and to only implement wider security subsequently. This section describes the steps to be taken if Core Protection is the chosen approach.

The security concept for the organisation will be drawn up after initiating an information security process, identifying the essential framework conditions as well as the processes, applications and IT systems to be protected and selecting an approach. For such purpose, organisational, personnel-related, infrastructural and technical standard security requirements are imposed in the IT-Grundschutz Compendium for typical components of business processes, applications and IT systems. These are classified in modules so that they can build on each other.

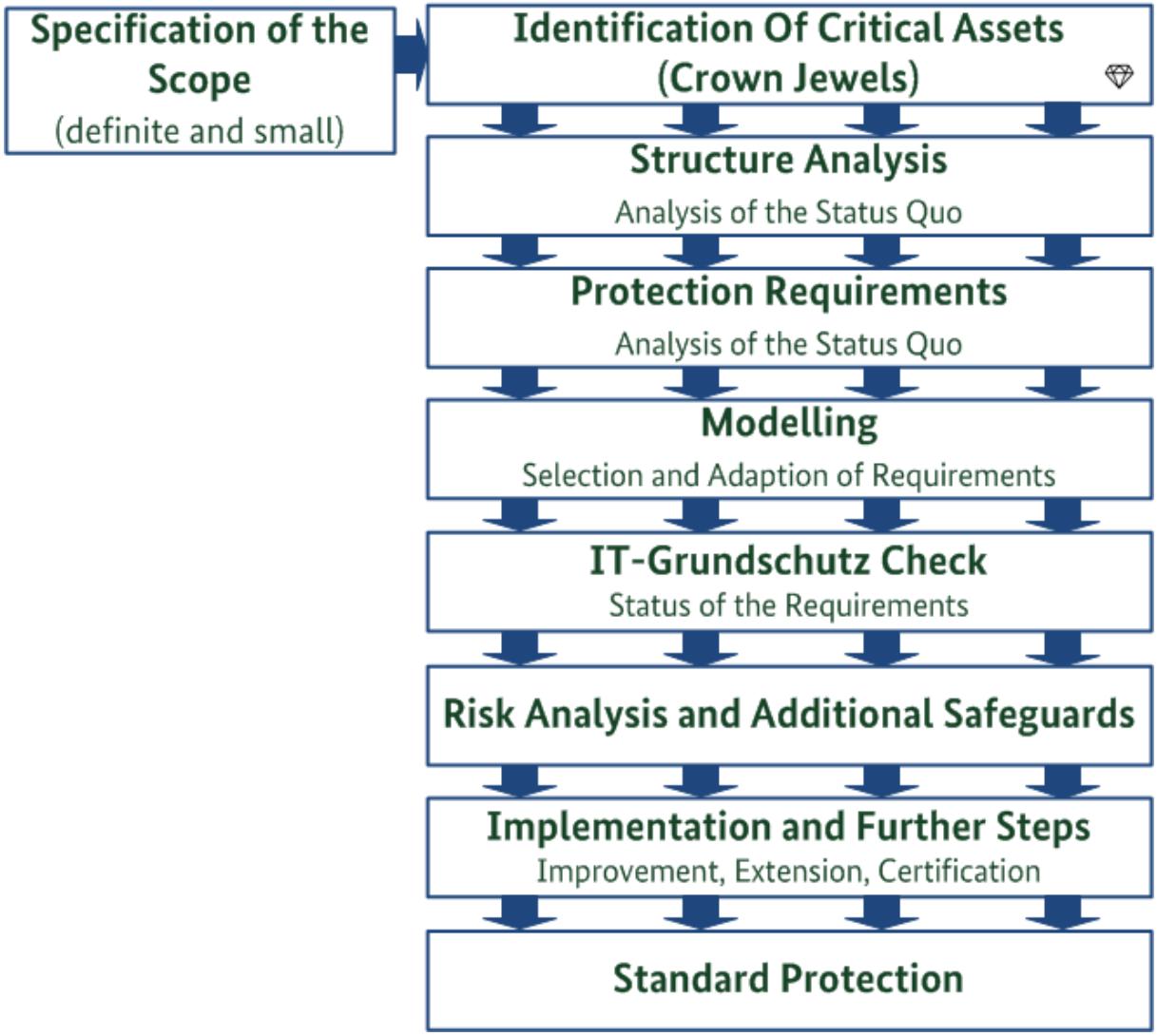


Figure 9: Core Protection

7.1 The methodology of Core Protection

The "Core Protection" approach of IT-Grundschutz focuses on the protection of assets requiring particular protection, the so-called "crown jewels". When using the Core Protection, a gap analysis between the requirements for safeguarding such crown jewels specified in the IT-Grundschutz

Compendium and such requirements fulfilled already in the organisation is made. Requirements that are found to be not fulfilled or inadequately fulfilled reveal security deficits that should be rectified by implementing corresponding measures.

The security concept drawn up using the Core Protection is the basis for a more comprehensive security concept as it can be drawn up and established using the Standard Protection (see Section 8).

As Core Protection focuses on the assets requiring particular protection, an increased protection need is to be assumed here basically. Thus, the basic and standard requirements specified in the relevant modules of the IT-Grundschutz Compendium must be implemented completely. Based on this, in case of increased protection need a risk analysis must be performed considering aspects of costs and effectiveness so that the relevant risks in the field of the crown jewels can be treated holistically. The requirements for increased protection need stated in the modules by way of example can be taken as a basis for adding corresponding individual measures.

In this regard, BSI-Standard 200-3 *Risk Analysis based on IT Grundschutz* describes a simpler methodology as compared to traditional risk analysis methods.

The Core Protection, which focuses on the protection of crown jewels, is no solitary project, but part of the security process. The Core Protection can only be considered to be a project if it will be integrated into Standard Protection subsequently. As long as this is not the case, the Core Protection process must be checked and improved regularly.

Drawing up of a security concept for Core Protection in accordance with IT-Grundschutz is roughly divided into the following areas:

- Specification of the scope for Core Protection
- Identification and determination of critical assets (crown jewels)
- Structure analysis
- Protection requirements determination
- Modelling: selection and adaptation of requirements
- IT-Grundschutz Check
- Risk analysis and additional security safeguards
- Implementation and further steps

7.2 Specification of the scope for Core Protection

Holistic implementation of information security (as performed with Standard Protection) in a single large step is frequently too ambitious. Many small steps and a long-term, continuous process of improvement without high initial investment costs often bring greater success. Thus, Core Protection focuses on the assets and resources of the organisation requiring particular protection. The overall situation of security should be improved continuously based on such selected and limited area of the organisation.

First, the area for which the security concept should be drawn up and implemented must be defined. This area comprises, amongst others, all (partial) business processes, applications, IT systems, infrastructures required for processing the particularly critical business processes and information. This possibly includes also ICS systems. In IT-Grundschutz, the considered scope of the security concept is generally termed “information domain”. Thus, the Core Protection considers an intentionally limited information domain.

For Core Protection it is particularly important to not only clearly delimit the information domain, but also to keep it as small as possible. Any further target object added to an information domain increases complexity of safeguarding. Thus, in case of doubt it can be more reasonable to operate the critical objects in small, manageable areas that are separated from the rest of the organisation. For example, it is more reasonable processing business-critical information in separated IT environments

and to accept corresponding inconveniences instead of linking the business processes requiring utmost protection to many applications from the customary office environment, thus being required to safeguard all networked components on the then required high security level.

7.3 Identification and determination of critical assets (crown jewels)

The business processes and information that are most important for further existence of the organisation are called crown jewels. It is important to specifically limit the possible amount of data worth of protection.

Usually, the critical assets include the following:

- Information that are substantial for successful performance of essential business processes.
- Information and business processes having a significantly increased risk potential regarding information security. This refers to confidentiality, integrity AND availability.
- Information and business processes whose theft, destruction, compromising or impairment means a damage that threatens the existence of the organisation and that should be preferentially protected.

The following characteristics of crown jewels help with identification and delimitation of the critical assets:

- Crown jewels are information or business processes, but no services, applications, IT systems or similar objects.
- The amount of information and business processes with significantly increased protection requirements is manageable and/or includes only a small part of all business processes of the organisation. Only a few assets stand out significantly against the mass of assets regarding their importance for specialised tasks and/or business activities and may cause high damage to the organisation.
- Crown jewels can also be available in formats that are not obvious at first sight: they can be single files, data collections, structured or unstructured information up to hand-written notes or talks, but also knowledge and abilities of individual employees can be included.
- Crown jewels often are information for which it seems to be desirable adding even higher categories to the available classification scheme.
- It is to be assumed that the protection need of the crown jewels and any resources in the information domain connected to them is at least “high”.
- The protection need of crown jewels may change in the course of time. here, a typical example includes information of product novelties or annual accounts.
- Regarding crown jewels, differentiation between various “owners” of the information is required frequently. These may have different roles and responsibilities. This particularly refers to responsibility versus accountability.
- The protection need of crown jewels even can be classified as being so high that the security officers are not granted the authorisations to inspect them by themselves, but are ordered to protect them.
- All elementary threats of the IT-Grundschutz Compendium are relevant: often, particular focus is on the attacker. Furthermore, causes such as environmental impacts or human wrong-doing must not be forgotten.

Usually, the management level specifies the assets that are crown jewels. The decision to classify certain information as crown jewels immediately results in the necessity to take adequate security safeguards for such information. Corresponding to the extraordinary protection need of the crown jewels, they are correspondingly comprehensive and tend to be costly and expensive. Specialists

responsible, security officers and other entities may propose to classify such information as crown jewels; the final decision must be taken by the management level.

Every organisation should elaborate for themselves individual examples of crown jewels to enable better categorisation. Moreover, examples for differentiating crown jewels from important information should be created. A few typical practical examples of crown jewels are given in the following:

- Details on upcoming business decisions, e.g. strategy papers for company acquisitions, financing plans.
- Details on product developments, e.g. background material on patent applications, design drafts etc.
- Information on locations of protected plants, endangered persons or secret systems.
- Administrative access data for servers (if not findable, no quick access will be possible).
- Cryptographic material, e.g. master key for cryptographic methods used throughout the whole organisation.
- Construction plans or product recipes.

Comment: The secret family recipe of a caffeine soft drink is an example of a “crown jewel” frequently discussed in public. If such recipe is disclosed (loss of confidentiality), this will result in a media hype; however, there will be no threat to the company’s existence, but this could even contribute to product advertisement. In this context it also becomes obvious that some crown jewels can be too “hot” to be valuable for an attacker or competitor. However, an unnoticed change of the recipe (loss of integrity) could result in severe damage to the company’s reputation. The complete loss of the recipe finally would result in standstill of production and, correspondingly, would be the most serious problem.

There can be crown jewels where focus is not on an individual process or object, but where the crown jewels are created by cumulation of important business-critical values. Example: In case of a publishing house, if the strictly confidential draft of the last volume of a successful book series becomes known to the public, this will be a serious security incident. However, if all data of the best-sellers planned for the business year are destroyed and publication of such best-sellers is prevented correspondingly, this may result in an economic catastrophe for the publishing house.

There can be crown jewels where highest availability is not to be provided by an individual process or object, but where availability of the production chain or even of the protective installations themselves is to be safeguarded. The processes for energy production in a nuclear power plant are a corresponding example for this.

7.4 Structure analysis

To draw up a security concept, and especially to apply the IT-Grundschutz Compendium it is necessary to analyse and document the interaction of the business processes, applications and existing information technology. Since IT systems today are highly networked, the network topology plan should be used as the starting point of further technical analysis. The following aspects must be considered:

- the applications operated for Core Protection in the limited information domain, and the correspondingly supported business processes,
- the organisational and personnel framework conditions for such information domains,
- the networked and non-networked IT systems belonging to the information domain,
- the internal and external communication links between the IT systems,
- the existing infrastructure.

The individual steps in the structure analysis are described in detail in Section 8.1 of this document in the form of actions to be taken.

7.5 Defining protection needs

The purpose of defining the protection needs is to assess the level of protection that is adequate and appropriate for the business processes, the processed information and the information technology used. In so doing, the damage to be expected is considered for each application and the information processed that could occur as a result of a loss of confidentiality, integrity, or availability. It is also important to realistically estimate the possible consequential damages. Experience has shown that it is best to divide the protection needs into three categories: "normal", "high", and "very high". Basically, in case of the assets requiring protection by means of Core Protection, protection needs of the categories “high” and “very high” are to be assumed. Nevertheless, the protection need of such few, particularly business-critical assets must be estimated in a dedicated manner.

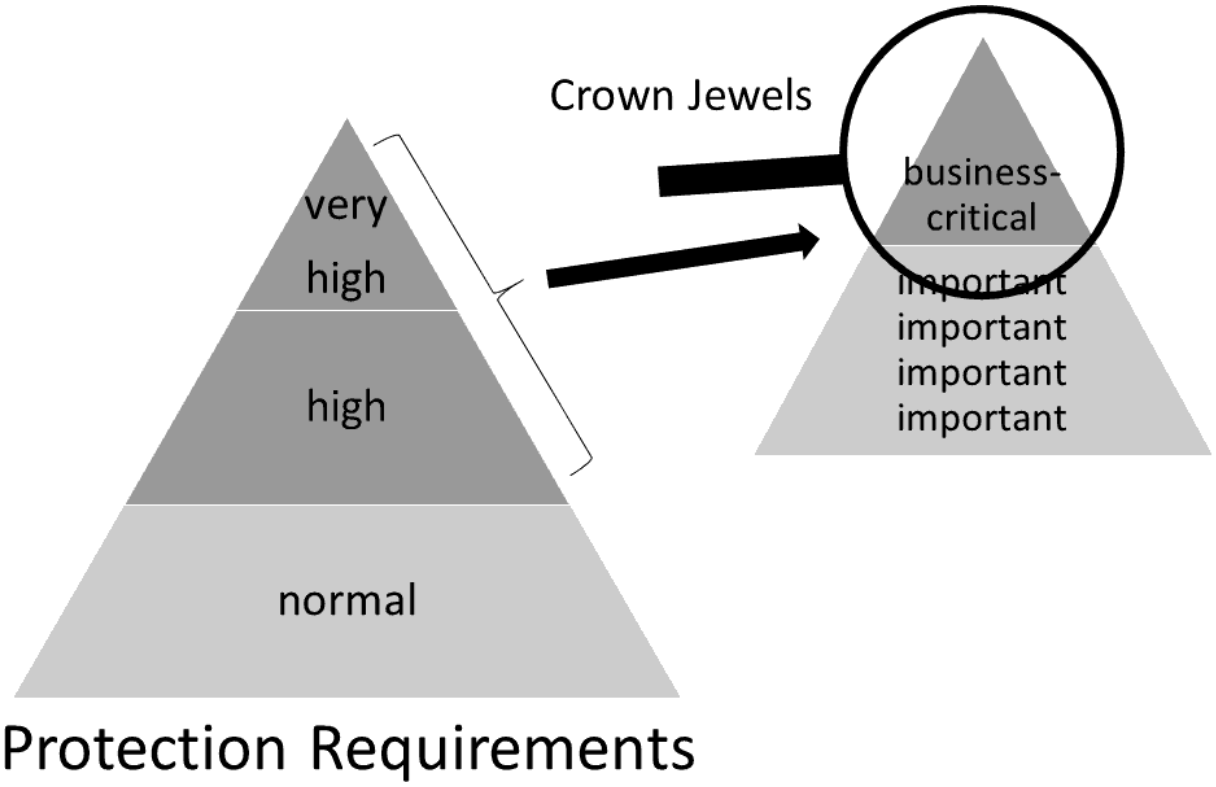


Figure 10: Protection need and crown jewels

In addition to the assets identified as crown jewels, typically there are further assets with high and very high protection need, also requiring appropriate protection.

The individual steps of defining protection needs are explained in detail in Section 8.2 of this document; however, it should be noted that Core Protection focuses on high and very high protection need.

7.6 Modelling: selection and adaptation of requirements

Detailed documents on the structure of the information domain and the protection needs of its included target objects are a prerequisite for application of the IT-Grundschutz Compendium. Such information should be determined by using the work steps described above. Then, the modules of the IT-Grundschutz Compendium should be mapped on the target objects and sub-areas to be able to identify suitable security safeguards for the present information domain.

This process of modelling is described in detail in Section 8.3.

7.7 IT-Grundschutz Check

The IT-Grundschutz Check is an organisational instrument providing a quick overview of the present level of security. Interviews are used to establish the status quo of an existing information domain (modelled in accordance with IT-Grundschutz) in relation to the extent to which the IT-Grundschutz security requirements have been fulfilled. The result is a catalogue where the fulfilment status “yes”, “partially”, “no” or “unnecessary” (with reasons, not possible in case of basic requirements) is documented for every relevant requirement. By identifying which requirements have not been fulfilled yet or have only been fulfilled partially, potential improvements regarding the security of the business processes being analysed and the information technology are indicated.

Section 8.4 describes an action plan for performing an IT-Grundschutz Check. This plan takes into account both organisational aspects and the technical requirements in the field of project implementation.

7.8 Risk analysis and additional security safeguards

Fulfilment of the standard requirements in IT-Grundschutz normally offers sufficient and adequate protection. In case of high or very high protection needs, as being regularly applicable within the scope of Core Protection, it should be verified whether there are additional security requirements, correspondingly requiring additional or, as an alternative, higher-quality security safeguards. This will also apply if there are certain conditions of use or if components that cannot be mapped using the existing modules of the IT-Grundschutz Compendium are used. Then it should be decided, whether risk analysis must be performed for the correspondingly affected areas to identify appropriate security safeguards.

One method for risk analysis is the approach described in BSI Standard 200-3 *Risk analysis based on IT-Grundschutz*. A summary of this methodology is provided in Section 8.5. The successful implementation of a risk analysis depends critically on the expertise of the project team. Therefore, it is frequently helpful to employ external specialists.

7.9 Implementation and further steps

The identified and consolidated security safeguards for Core Protection must be implemented subsequently. Section 9 *Implementation of the security concept* describes the things to be noted in this regard.

The tasks of an ISMS do not only include maintaining information security in the considered information domain, but also continuously improving the same (see Section 10). Regarding Core Protection this means that it must be checked regularly that the implemented security safeguards still correspond to the current threat scenario. Furthermore it should be considered that further areas of the organisation should be appropriately protected after successful safeguarding of the crown jewels. For this, e.g. the Basic or Standard Protection can be used for further areas, or the information domain of the Core Protection can be extended.

If the Core Protection has been implemented successfully in a delimited information domain, this can also be demonstrated internally and externally by means of certification in accordance with ISO 27001 on the basis of IT-Grundschutz. The steps required for this as well as the conditions to be fulfilled for successful certification are described in Section 11 *Certification according to ISO 27001 on the basis of IT-Grundschutz*.

8 Drawing up of a security concept according to the Standard Protection approach

One of the objectives of the Standard Protection of IT-Grundschutz is to offer a practical and effective approach to achieving a normal security level that can also provide 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 worked out. As a basis for this, the modules of the IT-Grundschutz Compendium include corresponding state-of-the-art security requirements for typical components of business processes, applications, IT systems, etc. These are classified in modules so that they can build on each other.

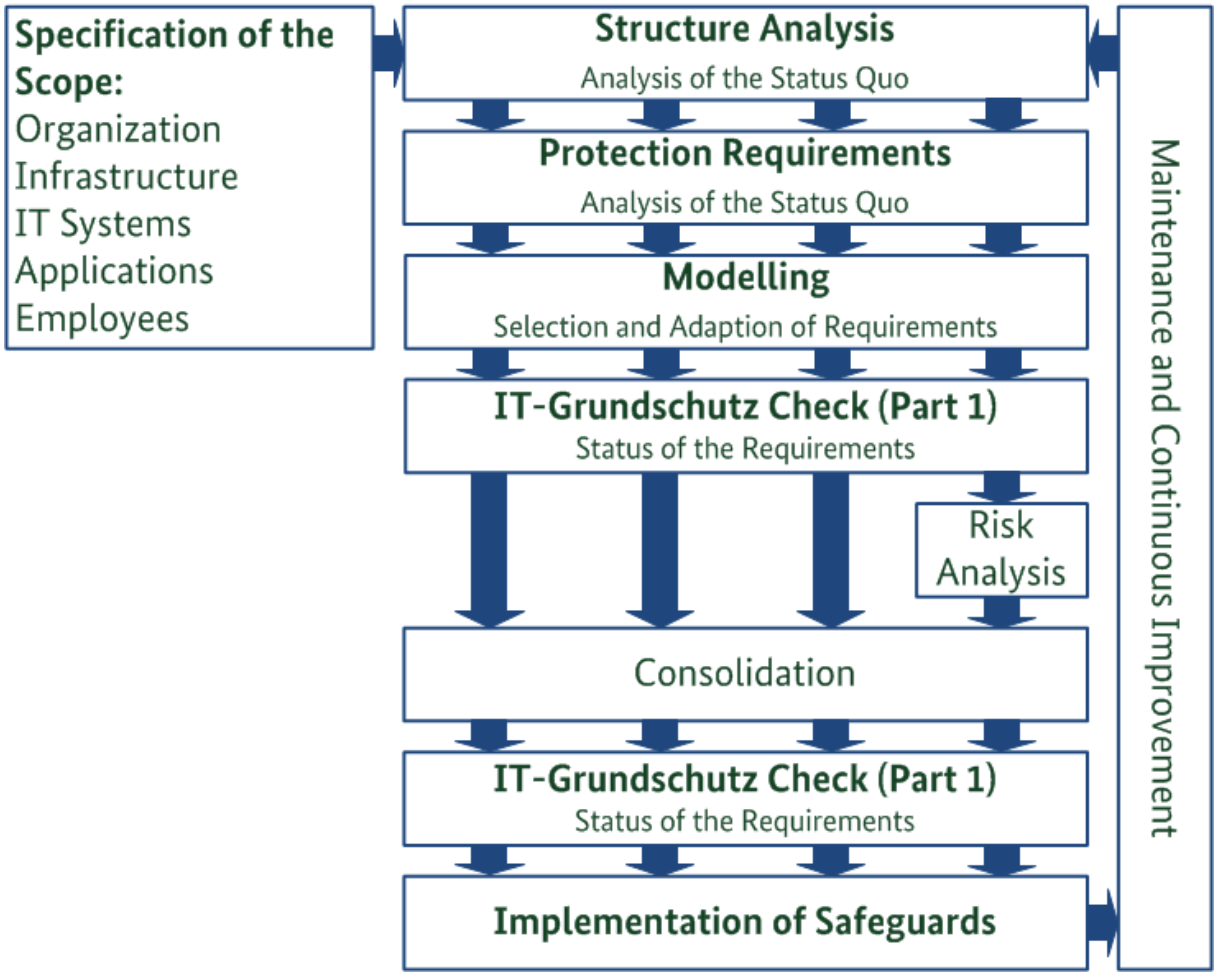


Figure 11: Drawing up of the security concept for Standard Protection

Implementation of Standard Protection in accordance with IT-Grundschutz is divided into the following fields of action:

Specification of the scope

When deciding on the further approach (see Section 3.3), also the scope for which the security concept should be drawn up and implemented has been specified. This may include e.g. certain organisational units of an organisation. However, this can also be areas processing defined business processes or specialised tasks, including the correspondingly required infrastructure. In IT-Grundschutz, the scope of the security concept is also termed “information domain”. The components to be safeguarded with the relevant modules of the IT-Grundschutz Compendium are parts of the considered information domain.

Structure analysis

To draw up a security concept in accordance with the Standard Protection approach, and especially to apply the IT-Grundschutz Compendium it is necessary to analyse and document the interaction of the business processes, applications and existing information technology. Since IT systems today are highly networked, which also applies to the fields of ICS and IoT, the network topology plan should be used as the starting point of further technical analysis. The following aspects must be considered:

- applications operated in the information domain and the correspondingly supported business processes,
- the organisational and personnel framework conditions for the information domain,
- the networked and non-networked IT systems, ICS and IoT components belonging to the information domain,
- the communication links in between and externally,
- the existing infrastructure.

The individual steps in the structure analysis are described in detail in Section 8.1 of this document in the form of actions to be taken.

Protection requirements determination

The purpose of defining the protection needs is to assess the level of protection that is adequate and appropriate for the business processes, the processed information and the information technology used. In so doing, the damage to be expected is considered for each application and the information processed that could occur as a result of a loss of confidentiality, integrity, or availability. It is also important to realistically estimate the possible consequential damages. Experience has shown that it is best to divide the protection requirements into three categories: "normal", "high", and "very high".

The individual steps in defining the protection needs are described in detail in Section 8.2 of this document.

Selection of requirements and adapting safeguards (modelling)

Detailed documents on the structure of the information domain and the protection needs of its included target objects are a prerequisite for application of the IT-Grundschutz Compendium. Such information should be determined by using the work steps described above. Then, the modules of the IT-Grundschutz Compendium should be mapped on the target objects and sub-areas to be able to identify suitable security requirements and safeguards to be implemented on the basis of such requirements for the present information domain.

This process of modelling is described in detail in Section 8.3.

IT-Grundschutz Check

The IT-Grundschutz Check is an organisational instrument providing a quick overview of the present level of security. With the help of interviews, the status quo of an existing information domain (modelled according to IT-Grundschutz) is determined in terms of the degree of implementation of the security requirements of the IT-Grundschutz Compendium. The result is a catalogue where the implementation status "unnecessary", "yes", "partially", or "no" is recorded for each relevant requirement. By identifying which requirements have not been fulfilled yet or have only been fulfilled partially, potential improvements regarding the security of the business processes being analysed and the information technology are indicated.

Section 8.4 describes an action plan for performing an IT-Grundschutz Check. This plan takes into account both organisational aspects and the technical requirements in the field of project implementation.

Risk analysis

Usually, appropriate and sufficient protection of an information domain is achieved by implementing the security requirements of the Standard Protection. However, if the protection needs are high or very high, it may be appropriate to check whether more stringent security measures are needed. This will also apply if there are certain conditions of use or if components that cannot be mapped using the existing modules of the IT-Grundschutz Compendium are used. In such cases a risk analysis is to be performed. It should be updated in regular intervals so that also changed threat scenarios are detected.

One method for risk analysis is the approach described in BSI Standard 200-3 *Risk analysis based on IT-Grundschutz*. A summary of this methodology is provided in Section 8.5. The successful implementation of a risk analysis depends critically on the expertise of the project team. Therefore, it is frequently helpful to employ external specialists.

Order of processing

The various activities required for drawing up of a security concept, i.e. structure analysis, defining the protection needs, modelling of an information domain, IT-Grundschutz Check, risk analysis, must not be necessarily processed successively. As far as possible on the basis of the present framework conditions and the size of the security team, they also can be performed independently from each other and simultaneously.

8.1 Structure analysis

The structure analysis is used to perform a preliminary survey of the information required for the further approach of producing a security concept in accordance with IT-Grundschutz. This means acquisition of the parts (business processes, information, applications, IT and ICS systems, rooms, communication networks) required for consideration of the scope.

Note: Frequently, the business processes are not acquired, not acquired consistently, or not acquired in the current state. Then, the relevant business processes must be identified first, e.g. by evaluating business distribution plans, descriptions of tasks, or other papers describing organisation.

For this, the business processes as well as the business-critical information and applications must be determined, and the affected IT, ICS or IoT systems, rooms and networks must be acquired. The classical approach is to first determine the applications and, based on this, the further affected objects. However, this approach has the disadvantage that it is often difficult to acquire abstract applications separately from concrete technical components. Thus, in some cases it may be reasonable, contrary to the order presented here, to first determine the IT and ICS systems because often the application can be determined more easily by using the considered systems.

It should be noted that the objects and data acquired within the scope of structure analysis are not only required for the security process, but also for operational aspects and for administration in most cases. Thus, it should be checked whether databases or summaries that can be used as data sources within the scope of the structure analysis are maintained yet. For example, many organisations operate databases for inventory, configuration management or designing of business processes. This may result in synergies.

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

- Acquiring of the business processes, applications and information belonging to the scope
- Determining a network plan
- Determining IT, ICS and IoT systems and similar objects
- Acquiring the rooms and buildings (for the ICS area also the producing rooms must be taken into account)

With all sub-tasks it is to be considered that often it will not be reasonable to acquire objects individually. Instead, similar objects should be combined in groups.

8.1.1 Reduction of complexity through the formation of groups

The structure analysis provides important basic data for the whole security process. The information domain is mainly composed of many individual objects that must be considered when designing. If all logical and technical objects are acquired individually, there will be the risk that the results of the structure analysis cannot be handled due to the amount of data and the complexity. Thus, similar objects should be reasonably combined in groups.

In case of technical components, consequent formation of groups also offers the benefit that administration will be simplified significantly if there are only a few basic configurations. Through the greatest possible standardisation within an information domain, the number of potential security gaps is also reduced and the security safeguards for this area can be implemented without differentiating the most varied of vulnerabilities. This not only benefits the information security, but it also reduces costs.

Objects may then be assigned to one and the same group if all the components

- are of the same type,
- have similar tasks,
- are subject to similar framework conditions, and
- have the same protection needs.

In case of technical objects, formation of groups will also be reasonable if they

- are configured similarly,
- are integrated similarly into the network (e.g. in the same network segment), and
- are subject to similar administrative and infrastructural framework conditions,
- operate similar applications, and
- have the same protection needs.

On the basis of the requirements stated for forming groups, it can be assumed for the information security that a sample of a group usually represents the security status of the group.

The most important example for grouping the objects is grouping clients. Organisations generally have a large number of clients that can however be classified in accordance with the scheme above into a clear number of groups. Also in producing and commercial areas it is recommended grouping objects if they are configured and used in a comparable manner (e.g. hand-held scanner, workstation PCs). This also applies correspondingly to rooms and other objects. In lathe information domains, where many servers perform the same task for reasons of redundancy or throughput, these servers can also be grouped together.

IT systems are virtualised increasingly. As this typically involves operation of many virtual machines (VMs) on a virtualisation server, reasonable structure analysis in case of virtualised infrastructures or cloud computing will only be possible by means if suitable grouping. For the formation of groups the same virtualisation rules apply as for physical target objects. In principle, also such VMs running on different physical IT systems can be grouped if they fulfil similar tasks, are configured similarly and have the same protection needs.

Usually, cloud computing platforms consist of homogeneous hardware and software components. Due to the homogeneity, a multitude of tasks can be performed centrally and in an automatised manner. Formation of groups, for example based on the protection needs, is absolutely necessary for cloud computing.

The sub-tasks of the structure analysis are described below and explained by means of an accompanying example. A detailed version of the sample is found in the auxiliary materials for IT-

Grundschutz on the BSI web pages. For all sub-tasks, objects should be grouped, respectively, if this is reasonable and allowed.

Action points on 8.1.1 Reduction of complexity through the formation of groups
• Form groups of similar objects for all sub-tasks of the structure analysis • Note the type and number of each of the grouped objects

8.1.2 Acquiring the business processes and the related information

One of the main tasks of the security management is to show the information security risks to the management level and to correspondingly create transparency regarding required decisions or actions. For this, the ISO must get an overview on the business processes and/or specialised tasks that are essential for the organisation, and must show the consequences of information security risks and/or IT risks for such business processes.

Thus, it is reasonable to create a relationship between the business processes and the value creation of an organisation and the information to be protected as well as the employed IT and/or the employed applications. For this, the business processes and their dependence on the most important applications must be documented.

In a first step, the business processes or specialised tasks included in the defined information domain are to be acquired and documented on the basis of such defined information domain. Here it should be ensured that reasonable granularity is selected. This means that not only an individual main process such as personnel management is acquired, but also the related sub-processes such as recruitment, employee administration, personnel development, etc. as far as these are part of the information domain. However, a documentation with a too high level of detail, e.g. by listing sub-sub-processes, should be avoided. Also in the field of ICS, structure analysis requires acquisition of the business processes together with the related information. Here, it should be particularly ensured that also further side processes such as the logistics processes for flow of goods and service/maintenance are taken into account in addition to the core process of production.

The individual processes are to be acquired as follows:

- Uniform identifier
- Name
- Person responsible for the process / specialised department
- Short descriptions of the processes or of the specialised task and the correspondingly processed information
- Important application(s) required for the processes

In many organisations, existing process maps can be used to identify the essential business processes. If the business processes have not been acquired, have not been acquired completely or have not been acquired in the current state, business distribution plans, task descriptions or other organisation-describing papers should be assessed first to identify the relevant business processes. In addition, the procedural directory of the Data Protection Officer can be a further starting point for acquisition of processes, specialised tasks and subsequent applications, even though this only maps the procedures and applications processing personal data. If no process descriptions are available, short workshops or interviews with the specialists responsible will be reasonable.

It can be reasonable to couple determination of the processes and specialised tasks to the determination of the applications to avoid redundant questions above all in the specialised departments.

Action points on 8.1.2 Acquiring the business processes and the related information
• Draw up a summary on the business processes • Label business processes with unique numbers or codes • Show correlation between business processes and applications

8.1.3 Acquiring the applications and the related information

In this phase, based on every business process and/or every specialised task, the related applications and the information processed with them must be identified. Applications are used for IT-technical support of business processes and specialised tasks in public agencies and companies.

The suitable granularity for the considered applications must be selected individually in each organisation. Here, the objective should be to achieve optimal transparency and efficiency of structure analysis and defining of protection needs. Also the modules of the application layer as considered in the IT-Grundschutz Compendium can give some indication for this step.

The structure analysis of the information domain can be limited to the applications and information that are required for the considered business processes or specialised tasks to further reduce the expenses. Here, it should be ensured that at least the applications and information that, based on the requirements of the considered business processes or specialised tasks, require a minimum level of

- secrecy (confidentiality) or
- correctness or genuineness (integrity) or
- availability

are taken into account.

When acquiring the applications, also the users and/or the persons responsible for the application as well as the persons responsible for the business processes should be asked how they estimate the required security level.

However, due to the increasing complexity of applications often the dependences between a business process or a specialised task and a concrete application are not clear to the specialists responsible. Thus, the applications required for performing a specialised task and the data accessed correspondingly should be determined for every single specialised task. These dependences can be acquired in a joint meeting of the specialised department, the persons responsible of the individual applications and the supporting IT department. For example, orders cannot be processed finally if information on the stock of inventory are not available.

If, contrary to the order presented here, the IT systems have been acquired first, often it will be helpful to collect the applications mainly on the basis of the IT systems. Due to their widespread impact, the servers should be the first items on which information is collected. In order to achieve as balanced a picture as possible, this determination can be completed for clients and individual workstation systems. Which network switching elements support which applications should then be established. Regarding acquisition of applications on a standard client, considering the standard software of the client as a package on behalf of the supporting IT department has proven to be successful in practice. Thus, the standard software will not be forgotten. Often, this is taken for granted and its application will not be stated explicitly in interviews any more (e.g. e-mail application or office communication).

The related business processes can also be acquired subsequently based on the applications (see section 8.1.2). The person responsible and the users of the application also should be acquired to be able to identify contact persons for security questions more easily and/or to be able to contact affected user groups quickly.

It is recommended to also consider data carriers and documents during acquisition and to handle them like applications. As far as they are not tightly linked to an application or an IT system, data carriers

and documents must be integrated separately into the structure analysis. Certainly, it will not be reasonable here to acquire all data carriers individually. On the one hand, only data carriers and documents with a minimum protection need should be considered, and on the other hand, groups should be formed as much as possible. Examples for data carriers and documents that should be acquired separately within the scope of structure analysis include

- archiving and backup data carriers,
- data carriers for exchange with external communication partners,
- mass-storage devices for mobile use (e.g. USB sticks or external hard drives),
- business continuity handbooks that are provided in printed form,
- microfilms,
- important contracts with partners and customers.

It must not be forgotten to also acquire virtualised applications within the scope of structure analysis.

It is recommended that the results are documented in tables or by using corresponding software products.

Example: RECPLAST GmbH

In the following the fictional organisation RECPLAST GmbH is used as an example to show how the acquired applications can be documented. It should be noted that the structure of RECPLAST GmbH is by no means optimal as regards information security. The example is simply used to illustrate the approach of using IT-Grundschutz. This document explains the individual activities for drawing up a security concept by using RECPLAST GmbH as an example. The complete example can be found in the Resources for IT-Grundschutz.

RECPLAST GmbH is a fictional organisation with approx. 500 employees, 130 of whom have their own workstations. The facilities of RECPLAST GmbH are separated into two sites within the city of Bonn, where the administrative and producing tasks are performed, amongst others, and three distribution locations in Germany.

All the workstations are networked in order to optimise the business processes. The Bonn branch office is linked to the headquarters over a leased line. The distribution locations are linked to the headquarters via secured Internet connections. Every employee can access via the Internet all policies and regulations essential for fulfilment of tasks and information security as well as forms and text blocks at any time. All the relevant products of the work are placed in a central database. Draft documents are exclusively prepared, distributed and signed in electronic form. Implementation and care of all required functions is performed by the IT department located in Bonn.

The business processes of RECPLAST are maintained electronically and are named on the basis of a two-level scheme. The number of the main process is added to the abbreviation GP, e.g. GP002. A business process should always be described so that a uniform understanding of delimitation of a process is present. Optionally, a process type can be documented. This is only used for reasons of providing a summary on the processes that mainly contribute to further existence of an organisation. The supporting processes are equally important; however, they are required rather for the general operation of an organisation.

The following includes an excerpt from the acquired business processes and the related information of RECPLAST GmbH:

A.1 Business Processes of RECPLAST GmbH				
Name	Process Description	Process Type	Responsible	Staff
GP001	**Production:** The production of plastics parts involves all steps between providing material and storing the final product. This contains internal transportation, production and assembly of different components and packaging of the final parts.	Core	Head of Production	All employees
GP002	**Proposal System**: Deals with customer requests for products. Usually customers send requests informally by e-mail or fax. Proposals are recorded electronically and sent to the customer by letter.	Supporting	Head of Proposal System	Sales
GP003	**Fulfillment:** Usually customers send orders by fax or e-mail. All receipts must be printed and recorded electronically. The customer only gets an order confirmation if he explicitly asks for it or if the production process differs from the usual production time.	Core	Head of Fulfillment	Sales
GP004	**Purchasing:** The purchasing department orders all articles that are not directly required for the production process. This department deals with external projects, IT contracts and consumable material like paper or toner cartridges.	Supporting	Head of Purchasing Department	Purchasing
GP005	**Disposition:** Here all materials required for production are purchased, e.g. screws or bags. Usually framework agreements are available. Disposition is planned according to yearly amounts and different order values.	Core	Head of Disposition	Disposition, Production

Figure 12: Excerpt from the business processes of RECPLAST GmbH

Structure analysis of applications:

In the structure analysis the responsible Information Security Officer of RECPLAST GmbH acquires the business processes and any further objects belonging to the organisation. This also includes applications required for maintenance of the business processes acquired already.

The following includes an excerpt from the acquired application and the related information for the fictional example of RECPLAST:

A.1 Structure Analysis of RECPLAST GmbH									
Name	Description of object (group)	Platform / Module	Location	Building	Room	#	Status	User	Responsible / Administrator
A003	**Word Processing, Spreadsheet:** An office software suite is used for all business information, e.g. business letters, analysis or presentations.	LibreOffice 6	-	-	-	130	operational	All employees	IT Services
A004	**Chat software:** A chat software simplifies communication between employees. By default, e-mails are read only twice a day. The chat software is being virtualized.	Standard Software	-	-	-	130	operational	All employees	IT Services
A008	**Active Directory:** Used as directory service to simplify user management.	Active Directory	Bonn	BG	Office	5	testing	Administrators	IT Services

Figure 13: Excerpt from the structure analysis of RECPLAST GmbH (applications)

The interaction between the business processes and the applications must be always shown. Ideally, such allocation should be performed by using tools in order to ensure clarity and up-to-dateness given the usual multitude of processes and applications.

The example of RECPLAST GmbH is used to show in the following that usually several applications can be used for a process:

A.1 Allocation of the business processes to the applications of RECPLAST GmbH										
Business Process / Application	A001	A002	A003	A004	A005	A006	A007	A008	A009	A010
GP001	x					x	x			x
GP002					x	x	x		x	
GP003					x	x	x		x	
GP004			x	x		x	x	x	x	
GP005			x			x	x	x	x	

Figure 14: Allocation of the business processes to the applications of RECPLAST GmbH

Action points on 8.1.3 Acquiring the applications and the related information
• Find out the applications required for the considered business processes by involving the responsible and/or the users of the applications • Draw up summary for the applications and label with unique numbers or codes

8.1.4 Determining a network plan

A network plan (for example in the form of a network topology plan) is a useful starting point for further technical analysis. A network plan is a graphical representation of the components used in the information and communications technology under consideration and of the manner in which they are networked together. Network plans or similar graphical summaries are available in most organisations also due to operational reasons. In detail, the plan should show at least the following objects with regard to information security:

- IT systems, i.e. client and server computers, active network components (such as switches, routers, WLAN access points), network printers etc.
- ICS and IoT components with network connection, i.e. clients, hand-held scanners, industrial printers, devices with programmable logic controller (PLC), control cabinets, etc.
- network connections between these systems, i.e. LAN connections (such as Ethernet), WLANs, backbone technologies (such as ATM), etc.
- connections between the area under consideration 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 sites, etc.

Moreover, for each of the objects represented there should be a minimum set of information which can be obtained from an assigned catalogue. As a minimum, the following information should be noted down for each IT system and other devices:

- 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),
- location (e.g. building and room number),
- the administrator responsible,
- the available communication interfaces (e.g. Internet connection, Bluetooth, WLAN adapter), and
- the type of network connection and network address.

In case of external connections or wireless communication links (WLAN, UMTS, LTE, etc.) additional details on the external network (e.g. Internet, business partner, name of provider of data transfer as well as type of line, e.g. MPLS, leased line, VPN) should be included.

Virtual IT systems (virtual switches, virtual servers, etc.) and virtual network connections such as virtual LANs (VLANs) or virtual private networks (VPNs) also should be presented in a network plan. In this, virtual IT systems must be treated according to their type and intended purpose, just like physical IT systems. Furthermore, the assignment of virtual IT systems to physical host systems must be comprehensible. In order to improve the clarity, it makes sense to divide the network plan into several partial network plans as the network size increases.

A cloud infrastructure consists of a number of elements. In addition to the physical (with CPU, internal memory and other hardware) and, if applicable, virtual servers this also includes networks and storage solutions. The stated areas usually have an administration software.

In the field of networks, the employed network management tools should support automatic creation of network plans. In addition to the physical IT systems, it also should be possible to automatically map virtual IT systems (e.g. virtual switches, virtual routers, virtual security gateways).

The ICS area can be operated as an autonomous network. When acquiring network connections also the interfaces should be acquired (list of allowed and blocked interfaces). Also the Internet connection out of the ICS area should be acquired. Separation of the networks between the office area and the ICS areas should be shown in the network plan.

Areas with different protection need should be marked. The network plan should be created and maintained in electronic form as far as possible. If the information technology in the organisation has gone beyond a particular size, it is appropriate to use a suitable programme to acquire and maintain the network plan as paper documents can be very complex and subject to constant change.

Updating the network plan

As the IT structure is generally adapted to the specific requirements of the organisation and maintenance of the network plan ties up certain resources, the network plan of the organisation will not always be up-to-date. In practice often only major changes in the IT structure of individual areas actually result in the plan being updated.

With regard to using the network plan for the structure analysis, the next step entails comparing the existing network plan (or partial plans, if the overall plan has been divided into smaller sections to make it easier to read) with the actual existing IT structure and if necessary updating it to reflect the current situation. During this activity, those responsible for IT and any administrators of individual applications and networks should be consulted. If any programmes are used for centralised network and system management, a check should be made in every case as to whether these programmes offer any support in drawing up a network plan. However, it should be noted that functions for the automatic or semi-automatic detection of components temporarily generate additional network traffic. Steps must be taken to ensure that this network traffic does not impair IT operations. Likewise, the result of automatic or semi-automatic detections always should be checked that all relevant components have been determined.

The area of industrial control also should be integrated into the network plan. In addition to the persons responsible for IT and the administrators, also the members of the building services teams are contact persons.

An adjusted network plan will also be helpful in other situations. It may be used to quickly show the business process and IT structures within the organisation to third parties because the level of detail is limited to the required extent in an adjusted network plan. An adjusted network plan is also a reasonable basis for certification.

Example: RECPLAST GmbH

The network plans at RECPLAST GmbH are administered at the IT department by using a tool. Presentation of all network plans is highly detailed and often quite confusing for third parties. That is why RECPLAST GmbH uses an adjusted network plan for presenting the acquired target objects.

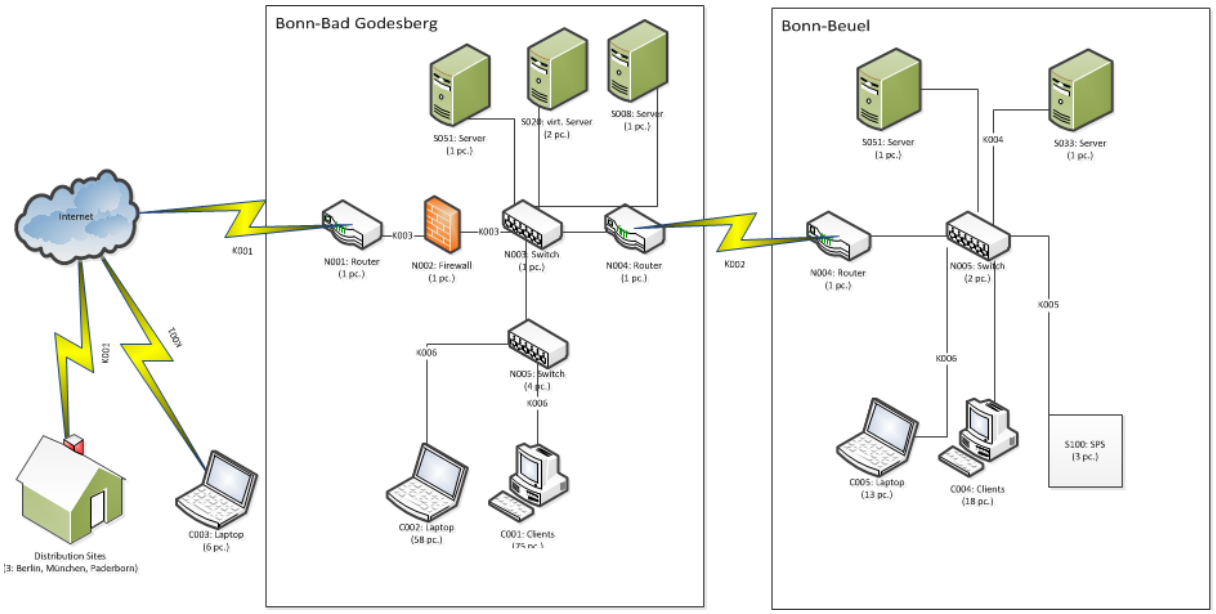


Figure 15: Excerpt from the adjusted network plan of RECPLAST GmbH (partial excerpt)

Action points on 8.1.4 Determining a network plan
• Sift through existing graphical depictions of the network, e.g. the network topology plans • If necessary update or produce network plans • Sift through existing additional information on the IT, ICS and IoT systems contained and, if necessary, update and complete • Sift through existing additional information on the communication links contained and if necessary update and complete

8.1.5 Determining the IT systems

With a view to defining the protection requirements and information domain modelling that are to be subsequently performed, a list of the existing and planned IT systems in tabular form should be produced. The term IT system does not only refer to computers in the narrower sense, but also to IoT and ICS devices, active network components, network printers, telecommunication systems, smartphones, virtual IT systems, etc. The focus is on the technical implementation of an IT system such as Apple MacBook, client in Windows, Linux server, telecommunication system, etc. Here, the systems should only be acquired as such (e.g. Linux server), but not the individual components that the IT systems are composed of (i.e. not computer, keyboard, monitor, etc.).

Note:

Proper IT operation requires complete and correct acquisition of the present and planned IT systems, e.g. for checking, servicing, troubleshooting and maintenance of IT systems. For drawing up of a security concept it will be sufficient to obtain an overview on the grouped IT systems.

Both the networked and non-networked IT systems, i.e. in particular those not incorporated into the network plan, are to be included. IT systems which have been grouped together in the network plan can be viewed from now on as a single object. Even IT systems that are not listed in the network plan must be checked to see whether appropriate groups can be formed. This may be possible for example for a large number of non-networked individual workstation PCs that meet the requirements in Section 8.1.1 *Reduction of complexity through the formation of groups*, and thus may be grouped together.

When acquiring the data, the following information which will be needed at subsequent stages should be noted:

- a unique identifier of the IT systems and/or the respective group (in case of groups also the number of summarised IT systems should be documented),
- description (e.g. function, type),
- platform (e.g. hardware architecture/operating system),
- place of installation of the IT systems (e.g. location, building, room),
- status of the IT systems (operational, in test stage, in planning stage), and
- users and/or administrators of the IT systems.

The applications are then in each case assigned to the IT systems which are necessary to run them. This can be the IT systems on which the applications are processed, but it could also include IT systems which transfer data generated within these applications. This results in a summary showing the relations between the important applications and the relevant IT systems.

Example: RECPLAST GmbH

A.1 Structure Analysis of RECPLAST GmbH

Name	Description of object (group)	Platform / Module	Location	Building	Room	#	Status	User	Responsible / Administrator
N001	**Router Internet Connection**: This router is responsible for communication between the internet and internal processes	Router / Switch	Bonn	BG	Server room	1	operational	Administrators	IT Services
N002	**Firewall Internet:** This firewall separates the internal network from the internet	Security Gateway	Bonn	BG	Server room	1	operational	Administrators	IT Services
N003	**Distribution Switch:** Responsible for data flow between internal network and internet	Router / Switch	Bonn	BG	Server room	1	operational	Administrators	IT Services
N004	**Router Bonn BG – Beuel**: These two sites are connected via a leased line	Router / Switch	Bonn	-	Server room	2	operational	Administrators	IT Services
S008	**Print Server:** Server for centrally managed print services	Server Windows 2012	Bonn	BG	Server room	1	operational	All employees	IT Services
S020	**Virtual Server (Configuration 1):** This server is able to host up to 20 virtual servers. Virtual systems are managed by dedicated software	Unix / Linux Server	Bonn	BG	Server room	2	operational	Administrators	IT Services
S033	**Production Server**: Central data for production is processed on this server.	Unix / Linux Server	Bonn	Beuel	Server room	1	operational	Production Department	IT Services

Figure 16: Excerpt from the structure analysis of RECPLAST GmbH (IT systems)

RECPLAST GmbH uses a tool for allocation of the applications to the IT systems because maintenance by means of a table is elaborate. Any change, whether with an IT system or an application, must be always documented. This allocation is required for subsequent determination of protection needs.

8.1.6 Determining the ICS systems

In organisation with production and manufacturing also the industrial control systems (ICS) used by the organisation must be documented.

Often, production and manufacturing uses a number of other devices in addition to IT systems. All ICS devices should be acquired correspondingly.

In the ICS area there are workstation PCs that should be grouped also here. Often, such PCs include the same applications like the office environment. Furthermore, special applications are installed on some PCs. Many PC workstations include a printer, and in addition to the standard peripheral equipment (mouse, keyboard) other peripheral terminal devices (e.g. hand-held scanner) directly connected to the workstation PC are used. The communication links (e.g. Bluetooth) of all peripheral terminal devices must also be taken into account.

Further terminal devices are used in the area of production and manufacturing. There are special terminal devices for industrial control, e.g. devices with programmable logic controls (PLCs), WLAN modules for industrial machines, self-driving forklift trucks (forklift vehicles).

When acquiring the ICS systems the following information which will be needed at subsequent steps should be documented:

- a unique identifier of the ICS systems and/or of the respective group of devices (the number of devices in the groups should also be documented),
- description (type and function),
- platform (e.g. operating system, type of (network) connection),
- place of installation of the devices (e.g. building, hall, room),
- status of the ICS systems (operational, in test stage, in planning stage), and
- persons responsible for operation of the ICS systems.

Example: RECPLAST GmbH

The following table lists examples of ICS systems:

A.1 Structure Analysis of RECPLAST GmbH

Name	Description of object (group)	Platform / Module	Location	Building	Room	#	Status	User	Responsible / Administrator
S100	**SPS:** Production facilities are programmed via SPS	SPS	Bonn	Beuel	Production	3	operational	Building Services	Building Services
S101	**SCADA:** This computer system is responsible for production process monitoring	SCADA / HMI	Bonn	Beuel	Production Hall	1	operational	All employees	Building Services
S103	**Server for acquisition of operational data:** Required for the BDE application. The server is connected to the production facilities	Unix / Linux Server	Bonn	Beuel	Server Room	1	operational	All employees	IT Services

Figure 17: Excerpt from the structure analysis of RECPLAST GmbH (ICS systems)

8.1.7 Determining other devices

Depending on the industry, organisations use various devices for supporting the business processes. In addition to IT systems, which are directly to be identified as such, also many other types of devices may affect information security. Such devices include, for example, devices with functions from the area of IoT.

Also devices such as air conditioning units, alarm systems or coffee machines that are not used for direct support of information processing or other business processes may affect the information security, e.g. if a burning cable results in consequential damage, but also if devices of such kind are integrated into the IT network for better control of resources.

Thus, the organisation should have an overview on what devices are used where, and which requirements on information security may result from this, such as regular checking of operational safety, servicing, or installation of patches.

IT-Grundschutz modelling should include acquisition of the devices with IoT functions that are networked, and particularly such devices that are not listed in the network plan considered above. Such devices should be grouped and handled as a single object as much as possible.

When acquiring the data, the following information which will be needed at subsequent stages should be noted:

- a unique identifier of the devices and/or the respective group (in case of groups also the number of summarised IT systems should be documented),
- description (type and function),

- platform (e.g. operating system, type of network connection),
- place of installation of the devices,
- status of the IT systems (operational, in test stage, in planning stage), and
- persons responsible for operation of the devices.

Internet of Things (IoT)

Frequently, IoT devices are characterised by that they have manageable, limited outer dimensions and often are below price limits resulting in an expensive purchasing processes in organisations, and/or that the Internet function is not prominent. Thus, it is probable that IoT devices are ignored in any kind of summary or inventory. It is important to get an overview on

- the IoT devices that are currently being used or will be used soon in the organisation, and
- the persons that typically use IoT devices in the organisation and to get talking to such persons.

Here, a reasonable approach for the ISO could be to go to the various rooms of the organisation and to identify the relevant components that require power and if they could be networked via IT networks. The ISO should talk particularly to the colleagues of the building services team, but also the other persons responsible for devices, and should get explained the functions of the various devices. Networking could be performed e.g. via IT cables or WLAN to the LAN, via mobile radio to the Internet, and also via fee WLANs in the environment or by using other radio interfaces such as Bluetooth. In addition, regular network scans should be performed to also search for devices that cannot be allocated.

Devices with IoT functions in organisations may include:

- Private devices brought along by employees or external persons, e.g. smartwatches, digital picture frames, weather stations, fitness wristbands, and other gadgets.
- Devices purchased and operated by the organisation such as fire, gas and other alarm systems, coffee machines or elements of building control. Here, the transition to ICS systems is seamless.

IoT devices cannot always be identified as such at first glance, e.g. if the IoT function is not a characteristic decisive for purchasing, but enables profitable data collection for the manufacturer, e.g. regarding type and quantity of consumables.

Examples of devices with hidden IoT functions include comfort furniture that automatically adapts to the respective use and stores the settings not only locally, but also exchanges them with other workstations via IT networks so that employees may work at any workstation (“smart workplaces”).

Example: RECPLAST GmbH

The following table lists examples of other and IoT devices:

A.1 Structure Analysis of RECPLAST GmbH									
Name	Description of object (group)	Platform / Module	Location	Building	Room	#	Status	User	Responsible / Administrator
S200	**Alarm System BG**: The alarm system for the site in Bad Godesberg is controlled by the reception	Alarm System	Bonn	BG	Reception	1	operational	Custodian	Building Services
S201	**Alarm system Beuel**: Basic system, used since 1996. Used for the site in Beuel	Alarm System	Bonn	Beuel	Reception	1	operational	Occupational health and safety practitioner	Building Services
S202	**Video Surveillance**: Cameras are watching all doors and some windows at the Bad Godesberg site. All emergency exits are also watched from the inside.	Unix / Linux Server	Bonn	Beuel	Server Room	1	operational	Reception	IT Services
S203	**Refrigerator IT Services**: IT Services owns a smart refrigerator that uses a camera and an app to provide an inventory list.	Refrigerator	Bonn	BG	Kitchen EG	1	operational	IT Services	Building Services

Figure 18: Excerpt from the structure analysis of RECPLAST GmbH (other and IoT devices)

Action points on 8.1.5, 8.1.6 and 8.1.7 Determining IT, ICS systems and other devices

- Check whether existing databases or summaries of the existing or planned IT, ICS systems as well as other devices are appropriate as the basis for the further approach
- Produce or update and complete list of networked and stand-alone IT systems, IoT and ICS devices
- Give IT, ICS, IoT systems or system groups unique names or codes
- Assign the applications to the IT, ICS, IoT systems (servers, clients, network switching elements, etc.) that are required for execution

8.1.8 Acquiring the rooms

The business processes and specialised tasks under review are not only operated on the defined IT systems but are also 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 on a shared floor. Many organisations use properties that are far apart or have to be shared with other users. Frequently, business processes and specialised tasks are also located in third-party rooms, e.g. within the scope of service contracts.

All properties in which the business processes and specialised tasks are operated must be included in a security concept. This includes the properties, buildings, floors, rooms and the routes between them. All communication links that pass through properties that are accessible to third parties must be considered external. This will also apply to wireless communication links if it cannot be excluded that they may be accessed by third parties. Rooms that are out of properties, but that are used occasionally or regularly for processing business processes or specialised tasks should not be forgotten. This also includes, for example, telecommuter workstations or temporarily rented workstations and storage areas.

For the further approach of modelling as per IT-Grundschutz and for planning the gap analysis it is useful to produce a summary of the properties, especially the rooms, in which the IT, ICS or IoT systems are located or are used for their operation. This includes rooms that are used exclusively for IT operations (such as server rooms, data media archives), those in which other IT, ICS or IoT systems are operated (such as offices or factory workshops) and also routes for communication links. If IT systems are stored in a protective cabinet instead of a special technical room, the cabinet is to be recorded as a room.

Note: When acquiring IT, ICS and IoT systems the installation location should have already been acquired.

In addition, checks must be made as to whether information that requires protection is stored in other rooms. Then these rooms must also be recorded. Here, also the rooms where non-electronic information requiring protection is stored, e.g. document files or microfilms, must be acquired. The type of information processed must be clear from this documentation.

Example: RECPLAST GmbH

The following section uses the example of RECPLAST GmbH to show how a table summary of the rooms could look like. Rooms can be grouped like all target objects. This will be possible as far as the rooms have similar equipment and comparable security requirements.

A.1 Structure Analysis of RECPLAST GmbH

Name	Description of object (group)	Platform / Module	Location	Building	Room	#	Status	User	Responsible / Administrator
R001	**Office:** A standard office contains desks, cabinets, cabling and so on. Offices can be locked. Each office can be used by one to six employees.	Office	Bonn	BG	-	27	operational	All employees	Facility Management
R002	**Meeting Rooms**: There are several meeting rooms at the Bad Godesberg site. Each contains desks, chairs, cabinets and cabling. Visitors are allowed in these rooms when supervised.	Meeting Room	Bonn	BG	-	5	operational	All employees	Facility Management
R003	**Work-at-home**: Some employees are allowed to work at home. The workplace must be protected against theft of company materials. The ISO examines the workplace with prior notice.	Telework	Mobile Working Place	-	-	27	operational	Teleworkers	ISB
R004	**Mobile Working Place**: All employees that use laptop/notebook for their work are allowed to freely choose their workplace, even outside of the RECPLAST buildings. Rules apply. Company documents may only be taken outside under strict guidelines.	Mobile Working Place	Mobile Working Place	-	-	75	operational	Executives, employees	IT Services

Figure 19: Excerpt from the structure analysis of RECPLAST GmbH (rooms)

Action points on 8.1.8 Acquiring the rooms
• Produce list of all properties, buildings and rooms listed when acquiring the IT, ICS and IoT systems • Add other rooms in which information requiring protection or processed in another manner are stored

8.2 Defining protection needs

The objective of defining the protection needs is to specify the protection needs of the acquired objects in the information domain regarding confidentiality, integrity and availability. These protection needs are oriented to the potential damage connected to adverse effect on the application affected and therefore on the corresponding business processes.

Defining the protection needs of the information domain entails several steps:

- Defining the protection need categories
- Defining the protection needs for business processes and applications
- Defining the protection needs for IT systems, IoT and ICS devices
- Defining the protection needs for buildings, rooms, factory workshops, etc.
- Defining the protection needs for communication links
- Conclusions from the results of defining protection needs

After defining the protection need categories, first the protection needs for business processes and the applications are defined using the typical damage scenarios. Then, the protection needs for the individual IT systems, rooms, and communication links are derived from this.

The corresponding approach is presented in detail in the following sections.

8.2.1 Defining the protection need categories

As the protection needs are not usually quantifiable, IT-Grundschutz restricts itself to a qualified statement by sub-dividing the protection needs into three categories:

Protection need categories	
"normal"	The effects of the damage are limited and manageable.
"high"	The effects of damage can be considerable.
"very high"	The effects of the damage can reach a catastrophic level that threatens the existence of the organisation.

Note:

It can also be reasonable for an organisation to define further categories. For example, downward grading can be introduced, e.g. "uncritical". (This can be defined as follows: "Damage to resources of the protection need category "uncritical" do not result in impairments or only in minimal impairments of the organisation.")

If only one or two categories are used, often the correspondingly achievable grading will not be sufficiently granular. However, if five or more protection need categories are used, clear differentiation between the individual stages will be more difficult. Furthermore, allocation of resources to one of the possible protection need categories is hardly understandable and this will result in increasing efforts both with allocation and auditing.

Another possibility is to use a category for confidentiality that is different from the categories for integrity or availability. For example, some organisation divide confidentiality into the categories "open", "internal", "confidential" and "secret", but integrity or availability only into "normal" and "critical".

If more than three protection need categories are defined, it should be considered which of the newly defined categories correspond to the protection need categories "high" and/or "very high" because such information are required for checking the decision on which objects to include into the risk analysis.

The following steps describe how to determine the appropriate protection needs category for business processes and the applications behind them.

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

- violation of laws, regulations or contracts,
- impairment of the right to informational self-determination,
- impairment of the physical integrity of a person,
- impairment of the ability to perform tasks,
- negative internal or external effects, and
- financial consequences.

Frequently, a single instance of loss or damage may involve several damage scenarios. Thus, for example, failure of an application could prevent essential work from being performed, resulting in direct financial loss and at the same time in a loss of reputation.

Note: Also the type and quantity of the considered scenarios can be adapted individually. Depending on the organisation there are different main topics that can be the focus of security management. Thus, the scenario of "Impairment of the right to informational self-determination" could be omitted if, for example, the data protection management already has been considering such scenario sufficiently in this organisation. In many organisations the scenario of "Impairment of the physical integrity of a person" can be omitted, unless this is a company where malfunctions of IT systems may result directly in personal damage. This could be the case e.g. in health care or in production areas.

Additional scenarios could also be considered, e.g.

- limitation of services for third parties or
- impacts on further infrastructures out of the own information domain (e.g. computing centres, IT operation of customer or service providers).

In order to differentiate between the "normal", "high" and "very high" protection need categories, it may be appropriate to determine the limits for individual damage scenarios. The following tables are used to determine the potential damage and its consequences for each of the protection needs. Each organisation must adjust the tables to its own situation.

"Normal" protection needs category	
1. Violation of laws/ regulations/contracts	• Violations of regulations and laws with minor consequences • Minor breaches of contract with at most low contractual penalties
2. Impairment of the right to informational self-determination	• It is a question of personal data, the processing of which may have adverse effects on the social standing or economic conditions of the person concerned.
3. Impairment of the physical integrity of a person	• Impairment does not appear possible.
4. Impairment of the ability to perform tasks	• The impairment would be assessed as tolerable by those concerned. • The maximum acceptable downtime is between 24 and 72 hours.
5. Negative internal or external effects	• Low and/or only internal impairment of reputation/confidence is to be expected.
6. Financial consequences	• The financial loss is acceptable to the organisation.

"High" protection need category	
1. Violation of laws/regulations/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	• It is a question of personal data, the processing of which may have significant adverse effects on the social standing or economic conditions of the person concerned.
3. Impairment of the physical integrity of a person	• Adverse effects on the personal integrity cannot be ruled out completely.
4. Impairment of the ability to perform tasks	• The adverse effects would be 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 reputation/confidence is to be expected.
6. Financial consequences	• The financial loss is considerable, but does not threaten the existence of the organisation.

"Very high" protection need category	
1. Violation of laws/regulations/contracts	• Fundamental violation of regulations and laws • Breaches of contract with ruinous damage liabilities
2. Impairment of the right to informational self-determination	• Includes personal data, the processing of which entails a danger to life and limb or the personal freedom of the person concerned.
3. Impairment of the physical integrity of a person	• Severe adverse effects on the personal integrity are possible. • Danger to life and limb
4. Impairment of the ability to perform tasks	• The adverse effects would be assessed as unacceptable by all concerned. • The maximum acceptable downtime is less than one hour.
5. Negative internal or external effects	• National adverse effects on the reputation or confidence are possible, which may even threaten its continued existence.
6. Financial consequences	• The financial loss threatens the existence of the organisation.

If individual considerations show that there are more than these six damage scenarios are possible, then they should be added. For all damage that cannot be depicted in these scenarios, it is also necessary to make a statement as to where the limit between "normal", "high" and "very high" is to be drawn.
Moreover, the individual circumstances which apply to the organisation should be taken into account: A loss of €200,000 could be relatively trivial when compared to the sales volume in a large company, but even a loss of €10,000 could threaten the existence of a small organisation. Therefore it often could be appropriate to express the limits as percentages of total sales, total profit, or on a similar base value.

Similar considerations apply as regards the availability requirements. Thus, for example, in some organisations a downtime of 24 hours could still be regarded as acceptable in the protection category "normal". But if several of these failures occur, e.g. more than once a week, the total may not be

tolerable. Thus, the availability requirements defined on the basis of the protection need categories should be specified if needed.

It can be necessary to define the protection need categories separately for the ICS area, but to adjust them on the basis of the protection need categories of the remaining information domain. For example, producing areas often make it necessary to define shorter downtimes for the corresponding categories as compared to the area of office IT. Time limits can be derived e.g. from maintenance contracts. Possibly, other elements must be adjusted, too. The protection needs must also be defined in data protection to be able to specify and configure appropriate technical and organisational security safeguards. The standard data protection model (SDM) provides a number of criteria to determine the risk of an infringement of basic rights and, consequentially, of the protection needs on the basis of three steps. The SDM also provides assistance if the protection needs do not agree from the point of view of information security and data protection.

When stipulating the limit between "normal" and "high", the fact that the IT-Grundschutz basic and standard security safeguards measures should be adequate for normal protection requirements should be considered. The stipulations made are to be appropriately documented in the security concept because the selection of security safeguards and therefore the consequential costs depend on this.

Action points on 8.2.1 Defining the protection need categories
• Consider typical damage scenarios for defining protection need categories • Define "normal", "high" and "very high" protection requirements categories, or adapt them to the own organisation

8.2.2 Procedure when determining the protection needs

First, the protection needs of the business processes and applications is determined. Then, the protection needs for the individual objects (e.g. IT systems, rooms, and communication links) are derived from this.

The protection needs of the business processes and the related information is the basis for determining the protection needs of various objects. The protection needs determined for them is inherited to the objects used for processing them, i.e. applications, IT systems, ICS and other devices, rooms and communication links (**inheritance**).

In order to define the protection needs of an object, the potential damage to the relevant partial objects must be considered in its entirety. For example, the effects of damage to applications run on an IT system and to the correspondingly processed information should be shown for an IT system. The damage or total damage with the most serious effects determines the protection needs of an object **(maximum principle)**.

When considering the possible damage and the corresponding consequences it also must be taken into account that the various considered objects of an information domain are closely connected to each other. For example, an IT application may use work results of other applications as input. A seemingly less important application A can assume significantly greater importance if another important application B depends on its results. In this case the protection requirements determined for application B must also be transferred to application A. If these are applications of different IT systems then the protection need requirements of the one IT system must be transferred to the other **(observing the dependencies)**.

If several applications and/or information are processed on an IT system (or in a room or via a communication link), it should be considered whether accumulation of several (e.g. smaller) damage events on one IT system may result in a higher total damage. This will increase correspondingly the protection needs of the object, i.e. of the IT system in the present case **(cumulative effect)**.

Example: All the applications of an organisation required for acquiring customer data are located on one network server. The damage in the event of failure of this applications was estimated to be low as there are sufficient alternatives. However, should the server (and thus also all applications requiring

such server) fail, the resulting damage would be considerably higher. Thus, it might be possible that fulfilment of tasks cannot be granted within the required time period. The protection needs of these "central" component should thus also be considered higher.

The opposite effect can also occur. Thus, it is possible for an application to have high protection needs, but its protection needs are not be passed onto an IT system under consideration because only insignificant parts of the application run on that IT system. In this case the protection needs have to be relativised **(distribution effect)**. As a matter of fact, the distribution effect may also occur with other target objects such as rooms, buildings and communication links.

Example: The distribution effect occurs mainly for the availability basic value. Thus, for example, where IT systems have been designed in a redundant fashion, the protection needs of the individual components may be lower than that for the entire application. Distribution effects are also possible for confidentiality: If it can be assured that a client only obtains uncritical data from a highly confidential database application, the client, in contrast to the database server, has just low protection needs.

A distribution effect often will occur if corresponding redundancies already have been used for considering the requirements on high protection needs when creating or developing target objects. Basically, this is an anticipation of considerations required within the scope of risk analysis. That is why the decisions taken within the scope of determining the protection needs should be documented properly.

Example: In case of applications having high protection needs regarding availability, redundancies have been considered already, e.g. alternative workstations in neighbouring buildings. The created distribution effects results in normal protection needs of these workstations regarding availability as long as there are sufficient alternative workstations available.

Definition of the protection needs is an **iterative process**. Rough definition of the protection needs is performed already in the very beginning, during the first discussion on the business processes and information and their impact on the organisation. Also after performance of risk analyses the determination of protection needs should be re-examined for possible adjustments because new knowledge on the protection needs of assets may appear during risk analysis and selection of safeguards.

8.2.3 Defining the protection needs for business processes and applications

For defining the protection needs in the various areas of an information domain, first the protection needs of the business processes and the relevant information must be determined. Based on this, the protection needs of the individual applications, IT systems, ICS and other devices, rooms and communication links is derived.

For determining the protection needs of the business processes, first the importance of the individual business processes for the organisation should be examined. This should be the basis for considering the dependences between business processes and applications, and how the correspondingly resulting risks can be mitigated. For this it proved to be successful discussing realistic damage scenarios together with the users based on the question "what if?", and to describe the material or sentimental damage to be expected. Often this also results in that critical dependences between business processes and further target objects not being focussed before are revealed.

The protection needs of the business processes result in the protection needs of the applications used for completing them.

Note: Suitable contact persons should be selected for estimating the protection needs; it will not be required to interview larger groups of users. For example, for evaluating the protection needs of certain central services such as DNS or e-mail it will be sufficient to have the protection needs being defined by the organisational unit that acts as service provider for the organisation (in most cases the IT department or the provider management). The protection needs of such services are to be communicated within the organisation. If individual specialised departments require higher protection needs of the services, possible solutions between specialised departments, security management and

the operator or provider of the service are to be discussed. Usually, an IT service provider may not provide its services for every possible protection need category. That is why the provider will offer its services with a protection need suitability defined by itself. When using a service for its business process, the owner of the information must decide if the protection need suitability offered by the IT service is sufficient or if additional security safeguards must be implemented due to the higher protection needs.

The definition of the protection needs must also include groups of data carriers and documents acquired in the structure analysis.

The appendix of this standard presents corresponding questions to simplify defining the possible damages and consequences. These suggestions do not claim to be complete; they are merely intended as a guide. If applicable, such questions must be amended and adapted to take into account the individual task and the situation of the organisation.

Determining the protection needs of the business processes and applications is a decision within the scope of risk management and often has far-reaching consequences on the security concept of the considered information domain. The protection needs of the business processes and applications is incorporated into determining the protection needs of the relevant technical and infrastructural objects such as servers and rooms.

In case of complex business processes, particularly if they have high or very high protection needs, it can be reasonable to divide them into sub-processes. If the area with high or very high protection needs can be limited to a few sub-processes, this will offer the benefit that the high and/or very high protection need will inherit to a few objects.

The results of defining the protection needs of the business processes and applications must be documented so that the results of defining the protection needs and the correspondingly resulting decisions within the scope of the information security management can be understood at any time later on. Care should be taken here to ensure that not only the assessed protection requirements are documented, but also the corresponding rationales. Later, these rationales will make it possible to check and further use the determinations.

Example: RECPLAST GmbH
The table below shows the main applications, their protection requirements and the rationales behind the assignment of protection requirements categories with regard to the company RECPLAST GmbH.

A.2 Protection needs of RECPLAST GmbH								
Name	Description of object (group)	Platform / Module	Confidentiality	Reason for confidentiality	Integrity	Reason for integrity	Availability	Reason for availability
A003	Word Processing, Spreadsheet	LibreOffice 6	normal	The application itself doesn't contain any information.	normal	The application itself doesn't contain any information.	normal	The application is installed on the client and can be reinstalled quickly. Outages of up to 24h are acceptable.
A007	Lotus Notes	Lotus Notes	high	The mailing system is used for confidential information. All e-mails are being signed.	normal	E-mails are not binding. Integrity is ensured by electronic signatures.	very high	The mailing system must be available even when other communication lines (like fax or phone) fail.
C002	Laptop in Administration	Windows 10 Client	normal	No information is stored locally on the clients.	normal	No information is stored locally on the clients.	high	Outages of up to 4h are acceptable.
G003	Sales Berlin	Building	high	Maximum principle: All kind of information is being processed in this building.	high	Maximum principle: All kind of information is being processed in this building.	high	Maximum principle: All kind of information is being processed in this building.
K001	Internet - Bonn BG	-	high	Maximum principle	high	Maximum principle	high	Maximum principle
R003	Worplace at home	Telework	high	Maximum principle	high	Maximum principle	high	Maximum principle
N001	Router Internet Connection	Router / Switch	high	The router connects the production network to the internet.	normal	Access is only possible for authorized personnel.	normal	Device can be quickly replaced, spare parts are available.
S020	Virtual Server (Configuration 1)	Unix / Linux Server	normal	Located in a server room with dedicated access control.	normal	Located in a server room with dedicated access control.	normal	Services are set up redundantly, so a failed server can be compensated by another one.

Figure 20: Excerpt from the definition of the protection needs of RECPLAST GmbH

At this point it may be appropriate to look beyond this information and consider the protection needs also from an overall view of the business processes or specialised tasks. This is appropriate for describing the purpose of an application in a business process or a specialised task and to derive its importance from it. This importance can be classified as follows:

The importance of the application is as follows with regard to the business process and/or the specialised task:

- **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 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.

The advantage of undertaking such a thorough assignment is, in particular, that management can regulate the protection needs for the individual applications when defining the protection needs. For example, it might be that a person responsible for an application views its protection needs as "normal"; whereas a manager might assess it more highly, given his view of the application within the wider business process or specialised task.

These optional data should also be documented by means of a table or using corresponding software products.

Action points on 8.2.3 Defining the protection needs for business processes and applications
• Define the protection needs of the acquired business processes and applications using the damage scenarios and lists of questions • Document the protection needs of the business processes and applications and their corresponding rationales in tables

8.2.4 Defining the protection needs for IT systems

In order to define the protection needs of an IT system, the applications that directly relate to the IT system must be considered first. A summary of the applications that are relevant for the various IT systems have been determined within the scope of the structure analysis (see Section 8.1). The protection needs of the business processes and applications (see Section 8.2.3) is incorporated into defining the protection needs for the correspondingly relevant IT systems. Here it must be ensured that not only the IT systems where the relevant application is installed are considered. Moreover, also the data flow of the application, which is used for inheriting the protection needs of the application to the intermediate network components, is to be considered.

In order to define the protection needs of the IT system, the potential damage to the relevant applications must be considered in its entirety. The results of defining the protection needs of IT systems should in turn be stored in a table. This should also list the protection needs that each IT system has for confidentiality, integrity and availability. The overall protection needs of an IT system are in turn derived from the maximum protection needs regarding the three basic values of confidentiality, integrity and availability. Therefore, an IT system will have high overall protection needs if one or several of the basic values has/have "high" protection needs. The protection needs of an IT system should be documented individually for all three basic values because this will typically result in various types of security safeguards.

For an IT system, for example, the overall protection needs may be high because the confidentiality protection needs is high but normal for integrity and availability. Thus, although the overall protection needs are high this implies that as a result the protection needs for integrity and availability have to be raised.

The determinations of the protection needs of the IT systems must be reasoned so that the decisions also will be understandable for persons not involved. In this case reference may be made to the definition of protection needs of the applications.

Example: RECPLAST GmbH
The results of defining the protection needs of the IT systems can be documented as follows (excerpt):

A.2 Protection needs of RECPLAST GmbH								
Name	Description of object (group)	Platform / Module	Confidentiality	Reason for confidentiality	Integrity	Reason for integrity	Availability	Reason for availability
N001	Router Internet Connection	Router / Switch	high	The router connects the production network to the internet.	normal	Access is only possible for authorized personnel.	normal	Device can be quickly replaced, spare parts are available.
N002	Firewall Internet Access	Security Gateway	high	Configuration must be kept confidential.	normal	Access is only possible for authorized personnel.	normal	Device can be quickly replaced, spare parts are available.
N003	Distribution Switch	Router / Switch	normal	Incoming data is sent to the correct recipient.	normal	Access is only possible for authorized personnel.	normal	Device can be quickly replaced, spare parts are available.
N004	Router Bonn BG - Beuel	Router / Switch	normal	Configuration must be kept confidential.	normal	Access is only possible for authorized personnel.	normal	Device can be quickly replaced, spare parts are available.
S008	Print Server	Server Windows 2012	normal	The server provides all printer drivers.	normal	Server monitoring can detect failures quickly.	normal	Can be reinstalled quickly as a virtual machine.
S020	Virtual Server (Configuration 1)	Unix / Linux Server	normal	Located in a server room with dedicated access control.	normal	Located in a server room with dedicated access control.	normal	Services are set up redundantly, so a failed server can be compensated by another one.
S033	Production Server	Unix / Linux Server	very high	The processed information is necessary for production. Lists of parts and work plans are stored in a database located on this server.	high	A permission concept is protecting the information stored on the server.	very high	The server must be available during production times (weekdays, between 6 am and 10 pm). There is no replacement server. Maintenance is carried out on weekends.

Figure 21: Excerpt from the definition of the protection needs of RECPLAST GmbH (IT systems)

Defining the protection needs in case of virtualised infrastructures

If virtualisation is used, defining the protection needs basically will remain the same. In order to determine the protection needs of an IT system, the applications that directly relate to the IT system must be considered first. In virtualised infrastructures usually several IT systems are operated on a virtualisation server. The protection needs of the applications are inherited to the virtual IT systems. The virtual IT systems inherit their protection needs to the virtualisation server. There are the following cases for the protection needs of a virtualisation server:

Confidentiality:

If the protection needs of the virtual IT systems are e.g. “normal”, then this will be inherited to the virtualisation server. Usually, it will also get the protection need “normal”. It should be considered whether accumulation of several (e.g. smaller) damage events on the virtualisation server may result in a higher total damage. In this case, the protection needs of the virtualisation server increase accordingly to “high” **(cumulative effect)**.

Integrity:

The protection objective of integrity will not be considered separately and is to be handled like confidentiality.

Availability:

If the protection needs of the virtual IT systems are e.g. “normal”, then the cumulative effect usually results in an increase of availability. At the same time, virtualisation offers the possibility of creating redundancies by using concepts like cold, warm or hot standby. Here, a replacement system is built up on another physical server in parallel to the productive system and either switched off (cold standby) or kept in such a state that it can be switched on, but is not used (warm standby) or switched on and supplied with data whilst being mirrored synchronously (hot standby). If corresponding safeguards are implemented, then the protection needs will decrease (**distribution effect**). Amongst others, the following cases may occur:

- The virtual machines have the protection need “normal” with regard to availability, then usually there is an accumulation to “high”, and then the protection needs decrease to

"normal" again due to distribution. In such case, the warm standby approach will be sufficient.

- The virtual machines have the protection need "high" with regard to availability. Due to accumulation, a very high total protection need may occur; this can be reduced to "high" due to distribution, if corresponding safeguards (e.g. hot standby) are implemented.

Defining the protection needs in case of cloud computing (IaaS compute)

Also in case of cloud computing there are only a few changes as compared to the definition of the protection needs as described above. In case of offers of the "IaaS compute" type virtual machines are provided to the users. e.g. via a web interface. Similar to virtualisation, the protection needs of the virtualisation server are influenced by the protection needs of the virtual IT systems operated on it. Techniques like Live Migration, vMotion or XenMotion make it possible that the virtual machines can be moved between the virtualisation servers or host systems can be switched to the standby mode or even shut down in case of low load to save energy. The benefits resulting from this are undisputed. However, Live Migration, i.e. moving VMs between virtualisation servers, makes it harder to define the protection needs. Thus, it is recommended to design the cloud computing platform for different areas (virtualisation clusters) based on the protection needs (e.g. "normal" or "high").

Then, applications having the same protection needs should be operated on a virtualisation cluster correspondingly provided for this. The individual areas should be physically separated from each other and it should be ensured that virtual machines cannot be moved across areas.

Special definition of the protection needs for virtual IT systems and virtualisation servers can be omitted.

Note: If most applications on a system only have normal protection needs and only one or a few have high protection needs, consideration should be given as to whether to export the applications requiring high protection to an isolated IT system as it is much more appropriate to secure this type of system; often it is also cheaper. Such an alternative can be presented to the management for decision.

8.2.5 Defining the protection needs for ICS systems

In the area of industrial control systems, the protection needs of all ICS systems must be defined. The ICS systems have been acquired in Section 8.1.6 and Section 8.2.5 already.

When defining the protection needs for the ICS systems it should be taken into account that not all objects automatically are subject to very high protection needs. It will be reasonable to perform definition of the protection needs in close consultation with the responsible persons of the ICS systems within the scope of a discussion because they know the requirements of the ICS devices regarding confidentiality, integrity and availability. Here, the protection needs are derived from the intended use of the industrial control system.

It should be considered that ICS systems can be used for various tasks. Thus, a production line alternately can produce product with high turnover that is important for the company and a product with less turnover. These dependencies must be considered when defining the protection needs (maximum principle).

Regarding the definitions of the protection needs it can be reasonable to take over the classifications defined for any other definitions of the protection needs. Moreover, the protection need categories can be formulated in a correspondingly adapted manner.

Example: RECPLAST GmbH

Regarding an IT system in a normal office environment, a downtime of up to 30 hours is within the normal range. Such downtime can also be reasonable for operation of ICS systems; however, it might be necessary to reduce the downtime for ICS devices with normal protection needs to 12 to 24 hours.

The protection needs for every ICS system are determined with regard to confidentiality, integrity and availability. The overall protection needs of the ICS systems are derived on the basis of the maximum principle with regard to the three basic values of confidentiality, integrity and availability.

The determinations of the protection needs of ICS systems must be reasoned briefly so that the decisions also will be understandable for third parties.

A.2 Protection needs of RECPLAST GmbH								
Name	Description of object (group)	Platform / Module	Confidentiality	Reason for confidentiality	Integrity	Reason for integrity	Availability	Reason for availability
S100	SPS	SPS	normal	Configuration can not be changed on the SPS directly.	very high	Configuration data must be correct all the time.	high	SPS must be available all the time, otherwise production stops.
S101	SCADA	SCADA / HMI	normal	A permission concept is protecting confidential information against unauthorized access.	high	A permission concept is protecting confidential information against unauthorized access.	high	Needed for processing production information.
S103	Server for acquisition of operational data	Unix / Linux Server	normal	Maximum principle	very high	Operational data must be correct all the time.	high	Outages of up to 7h are acceptable due to a buffer in production times.
S104	Server for acquisition of operational data	Unix / Linux Server	normal	Maximum principle	very high	Operational data must be correct all the time.	high	Outages of up to 7h are acceptable due to a buffer in production times.

Figure 22: Excerpt from the definition of the protection needs of RECPLAST GmbH (ICS systems)

8.2.6 Defining the protection needs for other devices

For defining the protection needs of other devices, first the business processes and applications for which these devices are used and how their protection needs are inherited must be determined. These Information have been determined in Section 8.1.7 and Section 8.2.6. Here, the data flow via such devices, which is the basis for inheriting the protection needs to the intermediate network components, must be considered.

In order to determine the protection needs of the device, the potential damage to the relevant business processes must be considered in its entirety. The results of defining the protection needs of devices should be documented in a table if such results have an impact on information security. Only devices that may have a noteworthy impact on information security should be considered in order to not being required to acquire any number of devices in an organisation. Such devices should be grouped and handled as a single object as much as possible.

The protection needs that each IT system has for confidentiality, integrity and availability should also be documented. The overall protection needs of a device are in turn derived from the maximum protection needs regarding the three basic values of confidentiality, integrity and availability.

The determinations of the protection needs of devices must be reasoned briefly so that the decisions also will be understandable for persons not involved. In this case reference may be made to the definition of protection needs of the business processes and applications.

Depending on the industry, organisations use various devices for supporting the business processes. In addition to IT systems, which are directly to be identified as such, also many other types of devices may affect information security. Such devices include, for example, devices with functions from the area of Internet of Things (IoT).

A.2 Protection needs of RECPLAST GmbH								
Name	Description of object (group)	Platform / Module	Confidentiality	Reason for confidentiality	Integrity	Reason for integrity	Availability	Reason for availability
S200	Alarm System BG	Alarm System	normal	Changes require special permissions.	very high	Data must be always correct since it is directly send to the local fire department.	very high	The alarm system protects the building and must be always available.
S201	Alarm System Beuel	Alarm System	normal	Changes require special permissions.	very high	Data must be always correct since it is directly send to the local fire department.	very high	The alarm system protects the building and must be always available.
S202	Video Surveillance	Unix / Linux Server	normal	Unauthorized persons must not get access to the video cameras	normal	Data must not be stored permanently and is only available for emergency cases.	hoch	Outages can be compensated by other means.
S203	Refrigerator IT Services	Refrigerator	normal	The stored data must not be changed.	normal	Stored data must be correct. The refrigerator is connected to a dedicated network.	hoch	During outages the refrigerator cannot be opened. Failure is tolerable up to 12 hours, afterwards the stored food is ruined.

Figure 23: Excerpt from the definition of the protection needs of RECPLAST GmbH (other and IoT devices)

Action points on 8.2.4, 8.2.5 and 8.2.6 Defining the protection needs of IT, ICS systems and other devices

- Determine protection needs of the IT, ICS systems and other devices on the basis of the protection needs of the business processes and applications
- Consider dependencies, the maximum principle and, if necessary, the cumulative or distribution effect
- Document the results for confidentiality, integrity and availability as well as the rationales for each system (group)

8.2.7 Defining the protection needs for rooms

The protection requirements for the relevant properties and/or and rooms should be derived from the results of defining the protection needs of the business processes and applications as well as of the IT systems, ICS and other devices. These protection needs are derived from the protection needs of the objects installed in the respective room, the information processed in the respective room, or the data carriers that are stored and used in such room, based on the maximum principle. Here, possible dependencies and the possibility of a cumulative effect should be considered, if a larger number of IT systems or ICS devices, data carriers, etc. are located in a room, such as is typically the case in server rooms, computing centres, factory halls or data carrier archives. A rationale should be documented for every estimation of protection needs.

Recording the necessary information in tables is also helpful for this and builds on the summary of rooms that was produced before.

Example: RECPLAST GmbH
The following table shows an excerpt from the results of defining the protection needs for the rooms of RECPLAST GmbH:

A.2 Protection needs of RECPLAST GmbH								
Name	Description of object (group)	Platform / Module	Confidentiality	Reason for confidentiality	Integrity	Reason for integrity	Availability	Reason for availability
R001	Offices	Office	normal	All offices have lockable cabinets. Employees must lock confidential material when leaving the office.	normal	Offices can be locked, there is no access for ousiders.	normal	There are enough offices available.
R002	Meeting Rooms	Meeting Rooms	normal	No documents are stored in meeting rooms.	normal	No documents are stored in meeting rooms.	normal	Meeting rooms are not used permanently.
R003	Work-at-home	Telework	normal	No confidential information is allowed at home.	normal	No confidential information is allowed at home.	normal	Only used infrequently. The regular working place is at RECPLAST offices.
R004	Mobile Working Place	Mobile Working Place	normal	No confidential information is allowed outside the office.	normal	No confidential information is allowed outside the office.	normal	Only used infrequently. The regular working place is at RECPLAST offices.

Figure 24: Excerpt from the definition of the protection needs of RECPLAST GmbH (rooms)

Action point on 8.2.7 Defining the protection needs for rooms

- Derive the protection needs of the rooms from the protection needs of the business processes, applications and IT systems, ICS and other devices
- Consider dependencies, the maximum principle and, if necessary, the cumulative effect
- Document results and rationales clearly

8.2.8 Defining the protection needs for communication links

After completing the definition of the protection needs for the considered business processes, applications, IT systems, ICS and other devices and rooms, the protection needs regarding the networking structure will be elaborated. The basis for further considerations is the network plan of the information domain under review as elaborated in Section 8.1.4 *Determining a network plan*.

To prepare the way for decisions as to which communication routes require the use of cryptographic security safeguards, which parts of the network should have built-in redundancy and over which connections attacks by insiders and external adversaries are to be expected, the various communication links must now be analysed. In this analysis, the following communication links should be regarded as critical:

- Communication links to the outside world, i.e. which lead into or through uncontrolled areas (e.g. to the Internet or over land to which the public have access). These may also be wireless communication links because it is difficult to prevent access to them on public property. For external connections there is a risk of penetration attempts by external attackers on the system that is to be protected or that malware could be installed. Moreover, an insider could possibly pass confidential information to the outside world over such connections. Also regarding the basic value of availability, external connections are often particularly at risk. Is must not be forgotten to also acquire external connections for remote administration.
- Communication links over which information that has high protection requirements is transmitted; this may include both information with high requirements on confidentiality as well as integrity or availability. These links could be targeted for wilful bugging or tampering. Moreover, failure of such a link could have a detrimental effect on the operational capability of significant numbers of the information domain.
- Communication links used in the producing area must also be acquired in the network plan. This includes (e.g. in case of separation of the network) the communication links between the networks.

One approach to gathering information about critical communication links is as follows. Initially, all “external connections” are identified and registered as critical connections. Then all the connections that are used by an IT system or a group of IT systems with high or very high protection requirements are examined. In this manner the connections over which information with high protection needs are

transmitted are identified. Subsequently, the connections used to transfer this highly sensitive data are examined. Finally, the communication links over which such information must not be transferred are identified. The information collected should include:

- the communications route,
- whether the connection has an outside connection, and
- whether information having high protection requirements are transmitted and whether the protection needs result from confidentiality, integrity or availability.

The decisions on which communication links are to be considered to be critical should be documented by table or should be highlighted graphically in the network plan.

Example: RECPLAST GmbH

Regarding the company RECPLAST GmbH, the communication links shown in the network plan in Section 8.1.4 *Determining a network plan* will apply. These have been grouped at RECPLAST on the basis of similar requirements as well as described and evaluated both in the structure analysis and in the definition of the protection needs. The following table can be used to understand the communication links shown above:

A.1 Structure Analysis of RECPLAST GmbH									
Name	Description of object (group)	Platform / Module	Location	Building	Room	#	Status	User	Responsible / Administrator
K001	**Internet – Bonn BG:** Internet connection for RECPLAST. Sales sites are connected to the central office via internet.	-	-	-	-	-	operational	All employees	IT Services
K002	**Leased Line Bonn BG – Bonn Beuel:** Connecting both sites in Bonn	-	-	-	-	-	operational	All employees	IT Services
K003	**Connections between network components inside RECPLAST**: All connections between routers, switches und firewalls with at least one protection need higher than normal.	-	-	-	-	-	operational	Administrators	IT Services
K004	**Connections between network components and servers inside RECPLAST**: All connections between network components and servers with at least one protection need higher than normal.	-	-	-	-	-	operational	Administrators	IT Services
K005	**Connections between network components and ICS, IoT and other devices inside RECPLAST**: All connections with at least one protection need higher than normal.	-	-	-	-	-	operational	Administrators	IT Services
K006	**Connections between network components and clients inside RECPLAST**: All connections with at least one protection need higher than normal.	-	-	-	-	-	operational	Administrators	IT Services

Figure 25: Excerpt from the structure analysis of RECPLAST GmbH (communication links)

A.2 Protection needs of RECPLAST GmbH								
Name	Description of object (group)	Platform / Module	Confidentiality	Reason for confidentiality	Integrity	Reason for integrity	Availability	Reason for availability
K001	Internet - Bonn BG	-	high	Maximum principle: Competitors might get access to confidential information.	high	A large part of communication is done via internet.	high	Maximum principle: This is a required external connection.
K002	Leased Line Bonn BG - Bonn Beuel	-	high	Maximum principle: Internal information must be transferred confidentially.	normal	Leased line is secured by internal measures.	high	Maximum principle: Without connection to the production site no orders can be processed.
K003	Connections between network components inside RECPLAST	-	normal	Internal connections can only be configured with access permissions.	normal	Internal connections can only be configured with access permissions.	high	Maximum principle: Components are required for internal network data flow.

Figure 26: Excerpt from the definition of the protection needs of RECPLAST GmbH (communication links)

Action points on 8.2.8 Defining the protection needs for communication links

- Acquire external connections and document them in tabular or graphical form
- Identify connections that are used to transfer critical information
- Document all critical communication links in tabular or graphical form

8.2.9 Conclusions from the results of defining protection needs

The results obtained from defining the protection needs serve as the starting point from which to proceed towards drawing up the security concept. Regarding the protection need categories, the following is assumed for protection that is based on the security requirements described in IT-Grundschutz:

Protective effect of security requirements according to IT-Grundschutz	
"Normal" protection needs category	Security requirements according to IT-Grundschutz are generally adequate and reasonable.
"High" protection need category	Security requirements according to IT-Grundschutz provide a standard level of protection, but may not be sufficient on their own. Additional safeguards should be determined on the basis of a risk analysis.
"Very high" protection need category	Security requirements according to IT-Grundschutz provide a standard level of protection, but generally are not sufficient. The required additional security safeguards must be determined individually on the basis of a risk analysis.

Except in case of high or very high protection needs, a risk analysis must also be performed if the objects of the considered information domain

- cannot be adequately depicted (modelled) with the existing IT-Grundschutz modules or
- are used in operating scenarios (environment, application) that are not planned in the scope of IT-Grundschutz.

For detailed information on risk analysis, see Section 8.5.

Areas with varying protection needs

When defining protection needs it is frequently the case that there are areas within the information domain under review in which information that has high or very high protection needs are processed. Even if only a few data items have higher protection needs, the strong networking and coupling of IT systems, ICS and other devices and applications rapidly leads to the higher protection needs being transferred to other areas using the maximum principle.

Thus, security zones for separation of areas with different protection needs should be created to limit risks and costs. Such security zones may be characterised in terms of rooms, technology or staff.

Examples:

- Geographical security zones: So that it is not necessary to permanently lock or monitor each individual office, zones having a lot of visitors should be separated from areas that have high protection needs. Therefore, meeting, training and event rooms, as well as the canteen that attract external customers should be located near the entrance to the building. Then it is possible for a gatekeeper to monitor access to the building parts that have offices. Particularly sensitive areas such as a development department should have additional access control, e.g. via chip cards.
- Technical security zones: In order to restrict confidential data to certain areas within a LAN and to prevent defects from affecting particular components or attacks on the functions, it is helpful to sub-divide the LAN into several sub-networks (see also module NET.1.1 *Network architecture and design* in the IT-Grundschutz Compendium).
- Employee security zones: Fundamentally each person should only be assigned the rights that are required to undertake their tasks. In addition, there are also various roles that one person should never undertake at the same time. For example, an auditor should not work in bookkeeping or in IT administration at the same time as he can and may not audit himself. In order to simplify the assignment of access rights, groups of people who perform functions that cannot be combined with each other should work in different groups or departments.
- Zone concept in case of virtualised infrastructures

  If virtualisation is used, then this should also be considered in the technical zone concept. Virtualisation means consolidation of the servers, i.e. the possibility to operate several servers virtually on a physical host. Here, the employed servers may be subject to different protection needs due to the applications and services running on them. Thus, the services and applications that are allowed to be operated together in a virtual environment and the services and applications to be separated by suitable measures should be specified before virtualisation. When performing segmentation it should be ensured that all areas of the IT infrastructure (“Servers”, “Networks”, “Storage” and “Management”) are acquired.

  The following should be taken into account when deciding which systems may be virtualised on a common physical hardware:

  - From organisational view and regarding security, the servers should be reasonably grouped in zones. Zones should not be virtualised together with the security component that is responsible for separation of the zones.
  - The components that can be jointly virtualised on a common physical hardware depend on the protection needs and the requester.

  Requesters may include different clients (hosting scenarios), different organisational units within a company or a public agency, or different procedures. In the first case, the challenge when planning is to achieve similar understanding by the requesters regarding the used protection need categories.
- Zone concept for cloud computing

In order to take into account the different protection needs of the users, cloud computing platforms must be multi-client capable and ensure reliable and continuous separation of users for the whole cloud computing stack (servers, networks, storage and management). In addition to the usual security safeguards such as malware and spam protection, IDS and IPS, suitable segmentation should be ensured on network level by defining and implementing security zones depending on the protection needs.

Examples of this include:

- security zone for cloud management
- security zone for live migration
- security zone for storage network
- security zones for virtual machines

Moreover, it is recommended implementing different zones for the server hardware based on the protection needs and to separate them from each other by using security gateways.

When planning new business processes, specialised tasks or applications it should be checked early whether it is reasonable to implement security zones. Frequently, this may save a lot of work during all subsequent phases until revision.

Action points on 8.2.9 Conclusions from the results of defining protection needs
• Check whether objects with increased security requirements can be concentrated in security zones
• Note objects with increased security requirements for a risk analysis

8.3 Modelling of an information domain

Once the required information is available from the structure analysis and the definition of the protection needs, the next step is to model the information domain under review with the aid of the existing modules of the IT-Grundschutz Compendium. This results in an IT-Grundschutz model of the information domain that consists of the various modules, possibly used several times, and contains the security-relevant aspects of the information domain due to use of the modules.

8.3.1 The IT-Grundschutz Compendium

The current version of the IT-Grundschutz Compendium (see [GSK]) can be downloaded from the BSI's web server.

The IT-Grundschutz modules

The IT-Grundschutz Compendium contains the threat scenario, security requirements and additional information for various procedures, components and IT systems, respectively summed up in a module.

In order to consider the additional investment and version changes above all in the IT area, the IT-Grundschutz Compendium has a modular design using the module structure and focuses on presentation of the essential security requirements for corresponding modules. Thus, it can be extended and updated easily. Based on the higher level, these modules are divided into process-oriented and system-oriented modules and grouped together in a layer model based on matching topics.

The process-oriented modules are grouped into the following layers:

- ISMS *(Information Security Management Systems)*
- ORP *(Organisation and Personnel)*
- CON *(Concepts)*
- OPS *(Operation)*
- DER *(Detection and Reaction)*

The system-oriented modules are grouped into the following layers:

- INF *(Infrastructure)*
- NET *(Networks and Communication)*
- SYS *(IT Systems)*

- APP *(Applications)*
- IND *(Industrial IT)*

Threats

First, the specific threat scenario to be expected is described in each module. Additionally, the separate appendix of the corresponding modules includes a list of fundamental threats considered when creating the module. This list of threats is part of the first level of the simplified risk analysis for typical environments of information processing and represents the basis on which the BSI compiled specific requirements for ensuring an appropriate level of information security in an organisation. The advantage of this is that the users are not required to use costly or further analyses for typical application cases in order to achieve the security level required for normal protection needs. Instead, it is sufficient to identify the modules relevant for the considered business processes and their required resources, and to consequently and completely fulfil the requirements recommended there.

Even if there are special components or application environments that are not adequately discussed in IT-Grundschutz, the IT-Grundschutz Compendium still provides a valuable aid to work. The risk analysis that is required then may focus on the fundamental threats of these components or environmental conditions.

Security requirements

Each module states the security requirements that are relevant for protection of the considered object. They describe *what* to do for its protection. The requirements are grouped into three categories:

- **Basic requirements** must be fulfilled preferentially because these recommendations may result in maximum benefit with (relatively) low efforts. These are unlimited requirements. The basic requirements are also the basis for the “Basic Protection” approach.
- **Standard requirements** are based on the basic requirements and address the normal protection needs. Basically they should be fulfilled, but not preferentially. The objectives of the standard requirements must be achieved to achieve Standard Protection. However, the corresponding framework conditions of the organisation may also result in reasons on why a standard requirement is not implemented as described, but the security objectives are achieved a different way. If a standard requirement is fulfilled by other security safeguards, the corresponding effects should be assessed carefully and documented in a suitable manner.
- **Requirements in case of increased protection needs** are a selection of proposals for further safeguarding that can be taken into account as a basis for elaboration of suitable requirements and safeguards in case of increased security requirements or under certain framework conditions.

The modules are addressed to security officers and persons responsible for security in organisations.

Implementation recommendations

There can be implementation recommendations in addition to the modules of the IT-Grundschutz Compendium. They describe how the requirements of the modules can be implemented, and they include corresponding security safeguards with a detailed description. The security safeguards can be used as a basis for security concepts, but should be adapted to the framework conditions of the respective organisation, if necessary.

The implementation recommendations respectively address the groups of persons that are responsible for implementation of the requirements from the modules, e.g. the IT operations or the building services. These implementation recommendations are provided for selected, above all highly requested topics.

8.3.2 Modelling of an information domain: selection of modules

Whether the information domain consists of already used components or whether it is an information domain that is fully or partially in the planning stages does not matter for the developed IT-Grundschutz model. However, the model may be used in different ways:

- The IT-Grundschutz model of an already implemented information domain identifies the relevant security safeguards based on the modules used. It can be used in the form of a **test plan** to perform a gap analysis.
- On the other hand, the IT-Grundschutz model of a planned information domain constitutes a **development concept**. Using the selected modules, it describes which standard safeguards need to be implemented when the information domain is implemented.

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

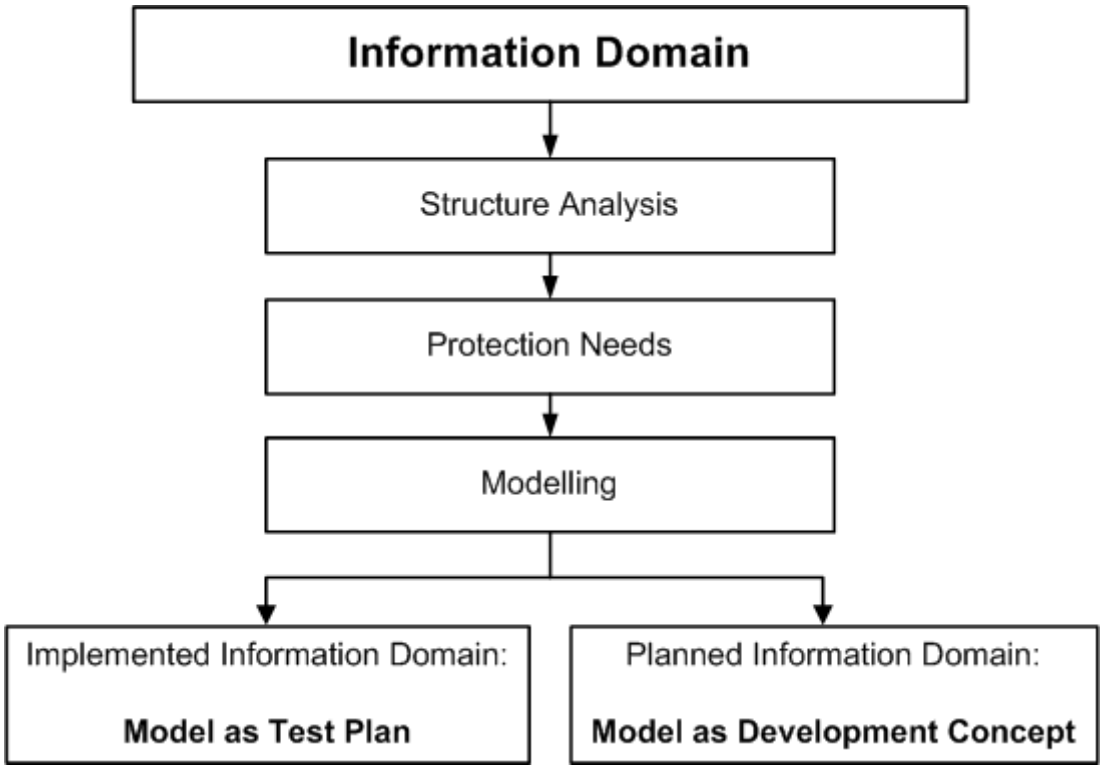


Figure 27: Results of modelling according to IT-Grundschutz

Typically, an information domain currently in use will comprise both implemented components and also components still in the planning stages. The resulting IT-Grundschutz model then contains both a test plan and some elements of a development concept. All security requirements envisaged in the test plan or development concept jointly form the basis for producing the security concept. In addition to the security requirements fulfilled already, this includes the requirements that were identified during the gap analysis as inadequate or not fulfilled at all, as well as those for the parts of the information domain that are still being planned.

The corresponding modules of the IT-Grundschutz Compendium must be selected and implemented to model a generally complex information domain according to IT-Grundschutz. In the IT-Grundschutz Compendium, the modules are separated into process-oriented and system-oriented modules and they are subdivided into individual layers to facilitate selection.

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

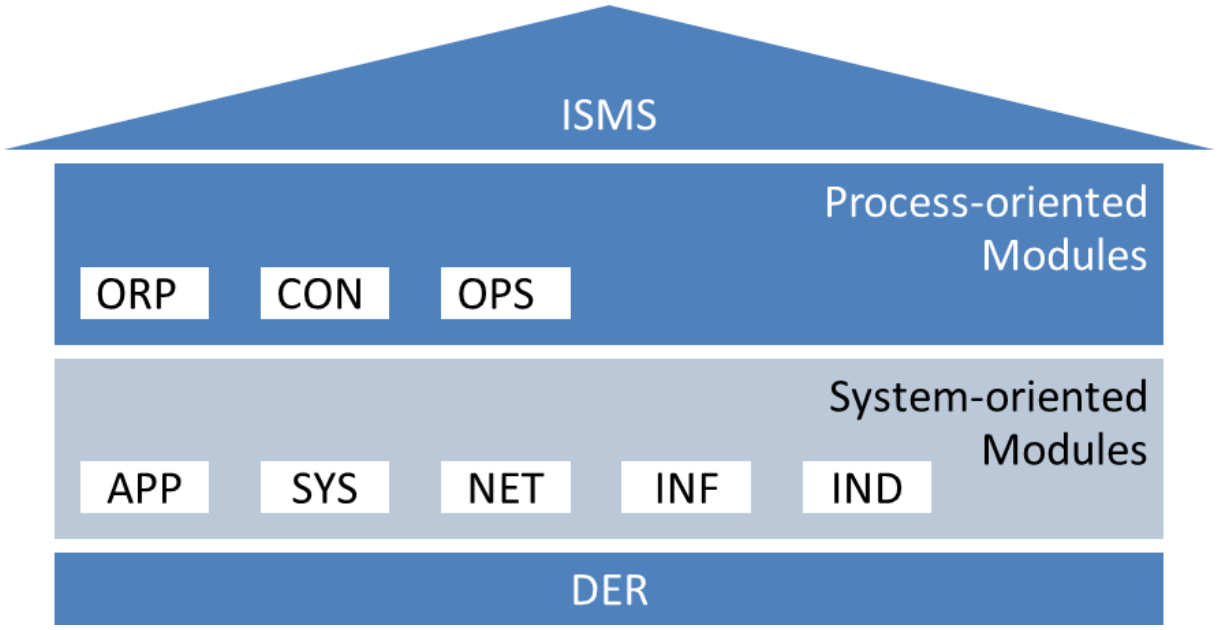


Figure 28: The layer model of IT-Grundschutz

Process-oriented modules:

- The ISMS layer includes the *Security management* module as a basis for all further activities in the security process.
- The ORP layer includes modules covering organisational and personnel-related security aspects such as the modules *Organisation* and *Personnel*.
- The CON layer includes modules dealing with concepts and procedures. Typical modules of the CON layer are, amongst others, *Crypto-concept* and *Data protection*.
- The OPS layer comprises all security aspects of the operational type. This particularly includes the security aspects of the operational IT operations both in case of in-house operations and IT operations that are run partially or completely at third parties. Furthermore, it includes the security aspects that are to be considered in case of IT operations for third parties. Examples of the OPS layer include the modules *Malware protection* and *Outsourcing.*
- The DER layer includes all modules that are relevant for checking the implemented security safeguards and particularly for detection of security incidents as well as the suitable reactions to them. Typical modules of the DER layer include *Handling of security incidents* and *Forensics*.

System modules:

- The APP layer deals with safeguarding of applications and services, amongst others in the areas of communication, directory services, network-based services as well as business and client applications. Typical modules of the APP layer include *Email/groupware*, Office products, *Web servers* and *Databases*.
- The SYS layer addresses the individual IT systems of the information domain that may have been divided into groups. Here, the security aspects of servers, desktop systems, mobile devices and other IT systems such as printers and telecommunication systems are addressed. The SYS layer includes, for example, modules for concrete operating systems, *Smartphones/tablet* and *Printers, copiers and all-in-one devices*.
- The NET layer examines the networking aspects not directly related to specific IT systems, but to the network connections and the communication. This includes, for example, the modules *Network management, Firewall* and *WLAN operation*.

- The INF layer addresses the architectural and structural factors; here, aspects of infrastructural security are brought together. This refers, amongst others, to the modules *Building and Server room / Technology room*.
- The IND layer deals with the security aspects of industrial IT. This layer includes, for example, the modules *Control room*, *Fieldbus* and *Control network*.

Using this layer approach has the following advantages:

- The complexity of information security is reduced because the individual aspects are divided up in a meaningful manner.
- Since higher order aspects and common infrastructural issues are considered separately from the IT systems, redundancies are avoided because these aspects only need to be dealt with once and not repeatedly for every IT system.
- The individual layers have been defined so that responsibilities for the aspects under consideration are grouped. The ISMS and ORP layers, for example, address fundamental questions regarding the secure handling of information, the INF layer the field of building services, the SYS layer the responsibility for IT systems, the NET layer the level of the network administrators and the APP layer finally the persons responsible for applications and those operating them.
- Breaking down the security aspects into layers enables individual subject areas within the resulting security concepts to be updated and expanded more easily without having a significant effect on other layers.

IT-Grundschutz modelling entails determining whether and how the modules of a given layer can be used to map the information domain. Depending on the module considered, there may be different types of target objects in the map: individual business processes or components, groups of components, buildings, properties, organisational units, etc.

8.3.3 Order of module implementation

The essential security requirements must be fulfilled early and corresponding security safeguards must be implemented to cover basic risks and establish holistic information security. Thus, IT-Grundschutz proposes an order for the modules to be implemented.

In the IT-Grundschutz Compendium, the Section *Layer model and modelling* describes when it is appropriate to use an individual module and which target objects it should be applied to. Furthermore, the modules are labelled with regard to whether they should be implemented with higher or lower priority.

- R1: These modules should be implemented preferentially because they are the basis for an efficient security process.
- R2: These modules should be implemented next because they are required for sustainable security in essential parts of the information domain.
- R3: These modules are also required in order to achieve the aspired security level and must be implemented; however, it is recommended, to only address them after the other modules.

Modules that are required for achieving a basic security structure are labelled with R1. These are modules of the following fields:

- ISMS *Security management*
- ORP *Organisation and Personnel*
- OPS.1 *Core tasks* of the *Own IT operations* layer

The modules to be implemented in the second and third step (R2 and R3) are present in all other layers of the IT-Grundschutz Compendium.

This label only shows the reasonable temporal order for implementation of the requirements of the respective module and does not represent an weighting of the modules with regard to each other. Basically, all modules of the IT-Grundschutz Compendium relevant for the corresponding information domain must be implemented.

Labelling of the modules only is a recommendation for an order of the various modules to obtain reasonable implementation. Here, every organisation may specify another order that is reasonable for such organisation.

8.3.4 Assignment of modules

The IT-Grundschutz modelling, i.e. the assignment of modules to target objects, should be documented in the form of a table containing the following columns:

- Number and title of the module
- Relevance: This column is used for deciding whether a module is relevant for the information domain to be modelled or not. It provides a quick overview to ensure that no module has been forgotten.
- Target object: If a module is relevant for the information domain, assignment to the target object and/or to a target object group is made via this column.
- Rationale: Incidental information and the rationale behind the modelling can be documented in this column. If modules for the considered information domain are not relevant, this should be explained here explicitly.
- Contact person: The concrete contact person is not determined at the modelling stage, but only at the point when the gap analysis in the IT-Grundschutz Check is being planned. However, based on the roles and responsibilities stated in the modules, preliminary work can be done here already.

Example: RECPLAST GmbH

The table below is an excerpt from the modelling performed for the company RECPLAST GmbH:

A.3 Modelling of RECPLAST GmbH				
Number and Title of the Module	**Relevance**	**Target Object**	**Rationale**	**Contact Person**
APP.1.2 Microsoft Exchange / Outlook	no		Not used.	
APP 3.6 DNS Server	yes	S019		
BD.1 Windows XP	yes	C002		
BD.4 Fax	yes	S005		
CON.6: Information security on trips abroad	no		Trips abroad are not relevant for the information domain.	
INF.1 General buildings	yes	G001		
INF.2 Computer centre and server room	no		There is no computer centre.	
INF.4 IT Cabling	yes	Information Domain		
ISMS (implemented requirements)	yes	Information Domain		
NET.1.1 Network architecture and design	yes	Information Domain		
NET.3.1 Router / Switches	yes	S033		
OPS.1.1.1 Proper IT administration	no		IT administration takes place outside of the information domain.	
OPS.2.4 Remote Administration	yes	Information Domain		
SYS.1.3 Unix / Linux Server	yes	S020		
SYS.4.1 Printers, copiers and all-in-one devices	yes	S048		

Figure 29: Excerpt from the modelling of RECPLAST GmbH

A detailed description of this approach for modelling of an information domain is included in the IT-Grundschutz Compendium in the Section *Layer model and modelling*.

8.3.5 Modelling for virtualisation and cloud systems

In general, the virtual IT systems are modelled according to the same rules as for stand-alone physical IT systems. This means that the information in Section 2.2 of the IT-Grundschutz Compendium must be taken into account. For IT components, the IT-Grundschutz modules are assigned primarily

according to the function of the IT system (i.e. as a server, client, etc.), the operating system used (Linux, Windows, etc.), and the applications running on the system (databases, web servers, etc.).

There are virtualisation software products requiring an underlying operating system (host-based virtualisation solutions), and others that are run on the physical hardware (bare metal virtualisation) without underlying operating system. If a full-featured and stand-alone operating system is operated below the virtualisation layer, then the corresponding module also must be assigned (e.g. from SYS.1.2 *Windows servers*) irrespective of the virtual IT systems.

If the hypervisor was installed directly on the physical hardware (bare metal virtualisation), this will represent a target object not included in the IT-Grundschutz Compendium as this is a very special target object. Thus, a risk analysis must be performed for the corresponding target object and the results must be consolidated with he requirements of the module SYS.1.5 *Server virtualisation*.

Exemplary scenario

As an example, we will consider a physical server S1 on which three virtual servers VM1, VM2, and VM3 are operated with the help of a virtualisation layer. A version of Linux is used as the base operating system on the physical server S1. The virtualisation layer in this example is a software component that runs on Linux, i.e. a host-based server virtualisation (type 2). The two virtual servers VM1 and VM2 are operated using Windows 2012, but Linux is installed on VM3. Applications can be run on the three virtual servers as well as directly on the base operating system of the physical server, Server S1 (by bypassing the virtualisation layer). The following figure shows a diagram of the configuration in this example:

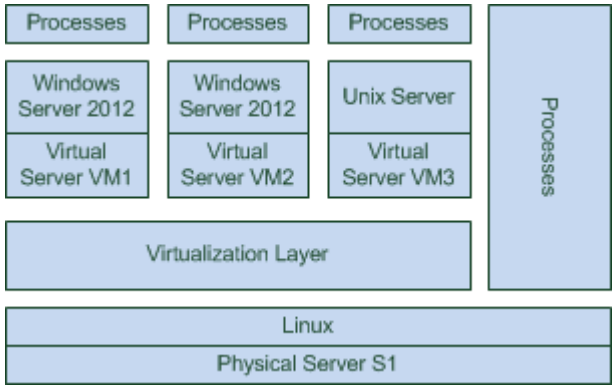


Figure 30: Scheme of an exemplary configuration

Module	**Target object**
SYS.1.1 *General server*	S1
SYS.1.1 *General server*	VM3
SYS.1.1 *General server*	Group with VM1 and VM2
SYS.1.3 *Unix server*	S1
SYS.1.3 *Unix server*	VM3
SYS.1.2.2 *Windows Server 2012*	Group with VM1 and VM2

Table: Assignment of modules of virtualisation layers to target objects

Modelling for cloud computing

In order to achieve an overall proper level of security for IT operations of cloud services, all cloud services (including their assigned virtual IT systems, networks, and additional cloud components) must be taken into consideration systematically within the framework of the security design. All IT systems, networks, and applications which are provided using cloud services and which are covered by the operational responsibility on the one hand and, on the other hand, by the scope of application of the ISMS of the cloud service provider must be taken into consideration within modelling according to the IT-Grundschutz approach. Here, the scope of application of the information domain can also be interpreted as the limit of responsibility: at the limit of responsibility, the responsibility of the cloud service provider ends and the responsibility of the cloud user starts. The extent of the information domain varies depending on the service model.

Modelling IaaS offers

Regarding IaaS (Infrastructure as a Service), the cloud service provider is responsible for the administration server for the cloud and the virtualisation server. Therefore, only the administration and virtualisation software are used as target objects for the APP (*Applications*) and SYS (*IT systems*) layers regarding IaaS. Thus, the corresponding modules must be selected for these. According to the IT-Grundschutz approach, these include modules for IT systems as servers (SYS.1 layer). The modules SYS 1.5 *Server virtualisation* and OPS.3.2 *Cloud providers* must be implemented for the cloud administration server.

Regarding IaaS, the cloud service provider merely provides a virtual “shell” using a virtual network. Regarding IaaS, the cloud service provider is responsible for securing the network according to IT-Grundschutz, whereas the cloud users are responsible for the IT systems of the cloud offer. For the network, suitable modules from the *Networks and communication* layer are to be modelled (e.g. NET.1.1 *Network architecture and design*). Normally, the virtual server is assigned a storage space from the storage network and module SYS.1.8 *Storage solutions / cloud storage* must also be implemented by the cloud service provider.

A virtual server from the cloud, offered via IaaS, is configured by the cloud user. The implementation responsibility regarding its security safeguards therefore also rests with the cloud user. As a consequence, regarding the delimitation of the cloud service provider’s information domain, this virtual server is outside of the cloud service provider’s information domain.

The interface for provisioning IaaS cloud services (self-service portal) must be secured by the cloud service provider using suitable mechanisms for network separation (e.g. by networks, virtual firewalls, routing) and, if required, module APP.3.1 *Web applications* must be implemented.

Modelling the IaaS servers as IT systems within the security design of the cloud service provider is possible, but not necessary, since the cloud users administrate these IT systems.

Modelling PaaS offers

Regarding PaaS (Platform as a Service), the cloud service provider, in addition to IaaS, is responsible for securely provisioning a virtual server and an offered platform (e.g. a database or a web server). Accordingly, the cloud service provider must initially model the cloud administration server and its administration software in the PaaS service model, as with IaaS. Module OPS.3.3 *Cloud providers* is assigned there in a centralised manner.

Furthermore, the cloud service provider must model an IT system with the corresponding operating system. For this IT system, a database or a web server must be modelled on application level depending on the cloud service.

The PaaS IT system with the connected cloud applications must be modelled for every cloud client, with the option of placing clients with the same platforms, applications, and protection requirements according to the specifications in Section 8.1.1 *Reduction of complexity through the formation of groups* together in one group.

In practice, cloud services of the PaaS service model are provided using virtual profiles that can be used for several cloud users and clients respectively. Therefore, it is useful in IT-Grundschutz modelling to model these combinations in the form of sample servers and to link and/or multiply these for every client.

Modelling SaaS offers

Regarding SaaS (Software as a Service), first the target objects relevant for the underlying cloud infrastructure must be identified like with IaaS and PaaS and assigned to corresponding modules.

When compared to PaaS, additional applications are modelled on the cloud IT systems regarding SaaS (e.g. a web service, a web application, or an SAP system). Regarding SaaS, in practice the cloud service provider is responsible for the whole cloud computing stack (servers, networks, storage, management, and applications). His/her field of responsibility also includes the SaaS applications so that they must be modelled within his/her information domain. In so doing, both multiple instances of the same SaaS application and groups of SaaS applications according to the specifications in Section 8.1.1 can be summarised if the prerequisites mentioned there are met.

8.3.6 Adapting module requirements

Modelling has been used to select the modules of the IT-Grundschutz Compendium that are to be implemented for the individual target objects of the considered information domain. The modules state the security requirements that are typically suited and appropriate for these components.

Now, for drawing up of a security concept or for an audit, the individual requirements must be processed and suitable security safeguards must be formulated based on this.

The requirements are concise and accurate. They stipulate partial targets that jointly contribute to implementation of the targets of a module. Thus, the security requirements still must be converted to action targets for the various actors in the security process. For this, security safeguards with the following characteristics must be elaborated based on the requirements:

- they must be adapted to the corresponding framework conditions and the terminology of an organisation,
- they must be sufficiently concrete for being usable in the present information domain, i.e. they must include e.g. sufficient technical details.

Generally, the requirements of the IT-Grundschutz modules always must be implemented analogously. All changes compared to the IT-Grundschutz Compendium should be documented so that the reasons can still be understood later.

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

The safeguards proposed in the implementation recommendations also should be adapted to the relevant framework conditions of an organisation. For example, it can be reasonable

- to further specify safeguards, e.g. by adding technical details,
- to adapt safeguards to the terminology of the organisation, i.e. by using other role names, and
- to delete the recommendations that are not relevant for the safeguards in the considered area.

All texts, modules, implementation recommendations, tables and aids are also provided electronically to make it easier for the users to adapt the IT-Grundschutz text to the target groups. Then, these texts can be used when drawing up a security concept and when implementing security safeguards.

When reviewing the security requirements it may occur that individual requirements cannot be implemented under the concrete framework conditions. This might be the case if the requirements in the considered environment are not relevant (e.g. if services have not been activated). In rare cases

this can also occur in the area of the unconditionally necessary basic requirements if their implementation would result in essential difficulties in other areas. This may be the case, for example, if fire control and intrusion protection requirements are incompatible. Then, other solutions must be found and this must be documented comprehensibly.

If security requirements are included or changed additionally, this must be documented in the security concept. This also simplifies performance of the IT-Grundschutz Check.

When selecting and adapting the security safeguards based on the requirements, it must be observed that they should always be appropriate. Appropriate means:

- Effectiveness: They must provide effective protection for the potential threats, i.e. they must cover the identified protection needs.
- Qualification: They must be able to be implemented in practice; they may not, for example, excessively hinder organisational processes or weaken other security measures.
- Practicability: They should be easily understandable, easy to use, and not prone to error.
- Acceptance: They must be usable for all users (barrier-free) and the must not discriminate or impair any person.
- Cost-effectiveness: An optimum result should be achieved with the resources used. On the one hand the security safeguards should minimise the risk as much as possible, and on the other hand they should be suitable for the values to be protected.

8.3.7 Involvement of external service providers

Many organisations use external or internal service providers or have business processes being performed by them partially or completely. Basically, involvement of external service providers can be performed in many ways, e.g. by means of personnel being used temporarily or by means of outsourcing of IT systems.

The tasks in the field of information security must be delimited and the interfaces must be specified in detail already before involving external service providers. Tasks can be outsourced to external service providers; responsibility for information security always rests with the outsourcing organisation.

The security-relevant tasks covered by the external service provider and the security-relevant tasks covered by the own security management must be clarified. The following questions should be clarified in detail before involving external service providers:

- Which business processes, IT systems or services should be outsourced to an external service provider?
- Which protection requirements do the target objects processed by an external service provider or within scope of outsourcing have?
- To which target objects and to which information does the service provider have access? On the one hand it should be considered which target objects and information are focussed by provisioning of services, but on the other hand it also should be considered which target objects and information can be accessed by the service providers, e.g. the cleaning staff's access to information in office rooms.

If an organisation opts for involvement of external service providers, both the contractual framework conditions and the prerequisites for implementation of the requirements of IT-Grundschutz must be met. In general, modelling of the modules must be performed separately with regard to the own organisation and any external service provider. The procedure of modelling is made as described in Section 8.3.4 *Assignment of modules*.

Also when involving external service providers, it must be possible for the outsourcing organisation to identify and control the risks in the field of information security at any time. Information and business processes must be always protected on a comparable level in accordance with the security

objectives of the organisation, even if they are performed partially or completely by external service providers (or their respective service providers). Furthermore, high transparency of events is required, i.e. there must be mechanisms ensuring that threats and risks that could have impacts on the services are detected and communicated.

For this, it is required to include security requirements as well as regular monitoring of meeting such requirements into the contracts.

When involving external service providers it is possible that the service provider is able already to provide a certificate for the involved service. Here, it must always be considered that the scope of application of the issued certificate actually includes the service.

Action points on 8.3 Modelling of an information domain

- Work through the Section *Layer model and modelling* in the IT-Grundschutz Compendium systematically
- Determine the target objects in the information domain under review to which each module in the IT-Grundschutz Compendium is to be applied
- Document the assignment of modules to target objects ("IT-Grundschutz model") and the relevant contact people
- Note target objects for a risk analysis that cannot be modelled appropriately
- Determining an order for implementation of the modules
- Carefully read security requirements of the identified modules and determine relevant security safeguards on such basis

8.4 IT-Grundschutz Check

The following considerations require drawing up the following parts of the security concept in accordance with IT-Grundschutz for the selected information domain:

A summary of the present business processes, the IT and its networking, the supported applications and the rooms was created on the basis of the structure analysis of the information domain. Then, based on this, the protection needs were assessed and the result of this was a summary of the protection needs of the business processes, applications, IT systems, used rooms used, and communication links. The information domain was modelled in accordance with IT-Grundschutz using this information. The result was a map of the information domain under review based on the IT-Grundschutz modules.

The modelling in line with IT-Grundschutz is now used as a test plan in order to discover which requirements have been fulfilled sufficiently or insufficiently using a gap analysis.

This section describes the recommended process for performing the IT-Grundschutz Check. The IT-Grundschutz Check consists of three different steps. The first step entails making the organisational preparations and in particular selecting the relevant contact people for the gap analysis. In the second step the gap analysis is performed using interviews and sampling checks. In the final step, the results of the gap analysis are documented, together with the rationale behind it.

The three steps of the IT-Grundschutz Check are described in detail below.

8.4.1 Organisational preliminary work for the IT-Grundschutz Check

A certain amount of preliminary work is required to ensure that the gap analysis proceeds smoothly. It is first necessary to inspect all the in-house documentation which controls security-relevant processes, e.g. organisational instructions, work instructions, security instructions, manuals and "informal" procedures. This also includes the documentation of the security safeguards implemented already. These documents can be helpful in ascertaining the degree of implementation, especially for questions

about existing organisational procedures. It is further necessary to clarify who is currently responsible for their content, in order to be able subsequently to determine the correct contact person.

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

Another step which needs to be performed before the gap analysis can be performed is to ascertain who are the appropriate people to interview. Initially, a main contact person should be stated for each individual module used to model the existing information domain. The requirements in the modules include the roles that are responsible for implementation of the requirements. Based on this information, the appropriate contact persons for the relevant subject matter in the organisation can be identified. The following shows some examples for contact persons of the various areas.

- For the modules in the ORP, CON and OPS layers a suitable contact person will generally be found by means of the subject matter dealt in the module. For example, for the module ORP.2 *Personnel* the contact person should be an employee from the responsible HR department. For the design modules, e.g. module CON.1 *Crypto-concept*, ideally the person who is responsible for updating the relevant document should be made available. Otherwise, the person whose terms of reference include updating procedures in the area under consideration should be interviewed.
- In the INF layer (*Infrastructure*) the selection of suitable contact people should be agreed with the internal services and/or building services departments. Depending on the size of the organisation being examined, different contact persons could be responsible, for example, for the two infrastructural areas of buildings and technology rooms. In small organisations the caretaker will often be able to provide the information. It should be noted that external departments should be involved in the area of infrastructure, if needed. This particularly applies to larger companies.
- In the system-oriented modules of the SYS, NET and IND layers the security safeguards to be checked increasingly deal with technical aspects. This means that generally the main point of contact will be the administrator for the component or group of components to which the module in question has been assigned during modelling.
- For the modules of the APP layer (*Applications*) people who support or are responsible for the individual applications should be selected as the main points of contact.

A schedule should be prepared to cover the interviews with the system administrators, administrators and other contact persons. Special attention should be given here to co-ordinating appointments with people from other organisational units or other agencies/companies. It is also appropriate to agree on alternative meeting dates.

Depending on the size of the project team, tasks should be allocated to different teams of interviewers. It proved to be successful to schedule two persons for performing the interview in every group. Here, one person asks the required questions and the other person takes down the results and remarks given by the interview partner.

Example: RECPLAST GmbH

Example: RECPLAST GmbH

A.4 IT-Grundschutz Check of RECPLAST GmbH				
Module	**Information Security Management**			
Requirement	**Description**	**Responsible**	**Status**	**Details**
ISMS.1.A1	Acceptance of overall responsibility for information security at the management level	Management	done	The management level has initiated and signed a policy for information security. The management level has accepted the overall responsibility for information security and delegated the implementation of safeguards to the appointed ISO. The management level gets monthly reports about the status of information security, controls the implementation of safeguards, initiates additional safeguards when needed and grants the needed budget.
ISMS.1.A5	Contract design when appointing an external Information Security Officer	Management	unnecessary	The ISO is an internal employee.
ISMS.1.A7	Definition of security safeguards	ISO	partly	All responsible employees must document the implementation of safeguards and inform the ISO via e-mail. There is not yet an evaluation of the documentation. Deadline for detailed documentation: April 30th.
ISMS.1.A11	Maintaining information security	ISO	done	There is a yearly internal audit for all documents and processes. The ISO has the necessary power to direct for all employees responsible for the respective documents and processes.

Figure 31: Excerpt from the IT-Grundschutz Check of RECPLAST GmbH (ISMS module)

Action points on 8.4.1 Organisational preliminary work for the IT-Grundschutz Check

- Sift through internal documents for responsibilities and rules and clarify who is responsible for these documents
- Determine to what extent external assistance is required
- Stipulate main contact person for all the modules used in the modelling
- Agree appointments for interviews
- Assemble team for interviews

8.4.2 Performing the gap analysis

Once all the necessary preliminary work has been completed, the actual survey can start at the times set. This entails progressively working through the security requirements contained in the module for which the person being interviewed is responsible.

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

"unnecessary" Fulfilment of the requirement in the proposed way is not necessary because the requirement is not relevant in the considered information domain (e.g. because services have not been activated) or has been dealt with by alternative safeguards.

If the implementation status of a requirement is set to “unnecessary”, then the relevant fundamental threats must be identified by using the cross-reference table of the corresponding module. If alternative safeguards have been used, it must be proven that the risk imposed by the relevant fundamental threats has been minimised appropriately. Generally it is to be considered that the occurring risk cannot be taken over in case of basic requirements.

Requirements must not be set to “unnecessary” by generally accepting or excluding the risk of a fundamental threat identified for a module by using the cross-reference table.

“yes"	Appropriate safeguards have been implemented completely, efficiently and appropriately for the requirement.
"partially"	The requirement only has been implemented partially.
"no"	The requirement has not been fulfilled yet, i.e. suitable measures have not been implemented yet to a large extent.

It is useful to have the module texts as well as the implementation recommendations or other supplementary material at hand during the interviews. The purpose of the IT-Grundschutz Check should be briefly presented to the interviewed persons. Continue by naming the requirement names and briefly explaining the requirement. The communication partner should be given the possibility to respond to the requirements and safeguards implemented already, and then unsolved questions should be discussed.

The questions asked should be always based on the level of basic and standard requirements, and any more far-reaching aspects of applications requiring high protection should be only considered after completion of the IT-Grundschutz Check. If it is necessary to verify the statements made in the interviews, this could be achieved, for example, by examining samples of the relevant rules and concepts; or in the case of infrastructure by visiting the objects under investigation on-site with the contact person, and/or by checking client and/or server settings in selected IT systems.

At the end of each module, the result should be provided to the interviewed persons (implementation status of the requirements: unnecessary/yes/partially/no) and such decision should be explained.

Action points on 8.4.2 Performing the gap analysis

- Prepare check-lists in advance for each specialised area
- Explain the objective of the IT-Grundschutz Check to the interview partners
- Ask for the implementation status of the individual requirements
- Verify answers using samples at the object
- Inform the interviewee of the results

8.4.3 Documentation of results

The results of the IT-Grundschutz Check should be documented such that all those involved can understand them, and they can be used as the basis for implementation planning for those requirements and measures where deficits still exist. The documentation efforts should not be underestimated. Thus, suitable aids providing support for drawing up and updating any documents required within the scope of the security process should be used.

This may include suitable IT-Grundschutz tools, i.e. applications supporting the whole approach according to IT-Grundschutz, from acquiring master data to defining the protection needs and risk analysis as well as gap analysis (IT-Grundschutz Check) to fulfilling the requirements. This provides convenient options for assessing and auditing the results, e.g. searching for particular entries, generating reports, analysing costs and statistical functions.

There are also forms available as additional aids for IT-Grundschutz. There is a file for each module of the IT-Grundschutz Compendium that can be used to record the results of the gap analysis in tables for each requirement in the module.

The following should be acquired for documentation of the IT-Grundschutz Check:

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

The actual result of the gap analysis should be included in a table. Here, the following information should be stated for each requirement of the respective module:

- Degree of implementation (unnecessary/yes/partially/no)
  The degree of implementation of the corresponding requirements as determined within the scope of the interview is to be recorded. Regarding possible certification the safeguards specifically fulfilling the requirements should be also recorded.
- Implementation until
  Such field is reasonable even though it is generally not filled in within the scope of an IT-Grundschutz Check. It serves as a placeholder which will be used during implementation planning to document the date by which the requirement concerned should have been fully implemented.
- Persons responsible
  If, when performing the gap analysis, it is clear which members of staff will be responsible for fully implementing a requirement or safeguard that is deficient, the name of this person can be documented in this field. If the person responsible is not clear, the field should be left blank. Then, a person responsible, whose name can be entered here, will be defined when further planning of implementation.
- Notes / reasons
  Such field is important to be able to understand any decisions later on, e.g. for certification. In the case of requirements whose implementation appears unnecessary, the rationale for this should be stated. In the case of requirements that have not yet been implemented or only partially implemented, this field should document which measures still have to be implemented. Any other notes which will assist in rectifying deficits or which need to be considered in the context of the requirement should also be entered here.
- Deficits / estimation of costs
  Regarding requirements not fulfilled or only partially fulfilled, the respectively connected risks should be determined and documented in a suitable manner. For example, this is important for audits and certifications. In case of such safeguards, the financial and personnel efforts for removing the deficits should be estimated.

Action points on 8.4.3 Documentation of results

- Acquire master information for every target object
- Document information on IT-Grundschutz Check and on the implementation status
- Include fields or placeholders for implementation planning

8.5 Risk analysis

A risk analysis within the scope of information security is to identify relevant threats for the information domains and to estimate the correspondingly resulting risks. The objective is to reduce

the risks to an acceptable level by using appropriate countermeasures, to the residual risks transparent, and to correspondingly enable systematic control of the overall risk.

Two-stage approach of IT-Grundschutz approach

When the approach according to IT-Grundschutz is used, a risk assessment is performed implicitly for areas with normal protection needs when drawing up the IT-Grundschutz modules. Only those threats which, after careful analysis, are shown to have such a high probability of occurring or such drastic consequences that security safeguards must be taken are considered. Typical threats that everyone must protect themselves against include, for example, damage due to fire, burglary, malware and hardware defects. This approach has the advantage that IT-Grundschutz users do not have to carry out an individual threat and vulnerability analysis for a major part of the information domain, since this assessment has already been performed in advance.

In certain cases, however, an explicit risk analysis must be carried out, for example if the information domain considered includes target objects which

- have high or very high protection needs in at least one of the three basic values of confidentiality, integrity or availability, or
- cannot be adequately depicted (modelled) with the existing IT-Grundschutz modules or
- are used in operating scenarios (environment, application) that are not planned in the scope of IT-Grundschutz.

In these cases, the following questions arise:

- Which threats for data processing are not adequately allowed for, or are not even factored in at all, in the implementation of the IT-Grundschutz modules?
- Might it be necessary to schedule and implement supplemental security safeguards over and above the IT-Grundschutz model?

For answering such questions, BSI recommends using a risk analysis on the basis of IT-Grundschutz as described in BSI-Standard 200-3.

The standard shows how to determine for specific target objects whether and in what respect there is any need to take action over and above the IT-Grundschutz in order to reduce risks for information processing. For this, risks assuming fundamental threats are estimated and assessed on the basis of a matrix. The estimation is carried out using the probability of occurrence and the extent of damage resulting when the damage occurred. The respective risk is derived from these two parameters. The methodology can be integrated into the IT-Grundschutz process as follows:

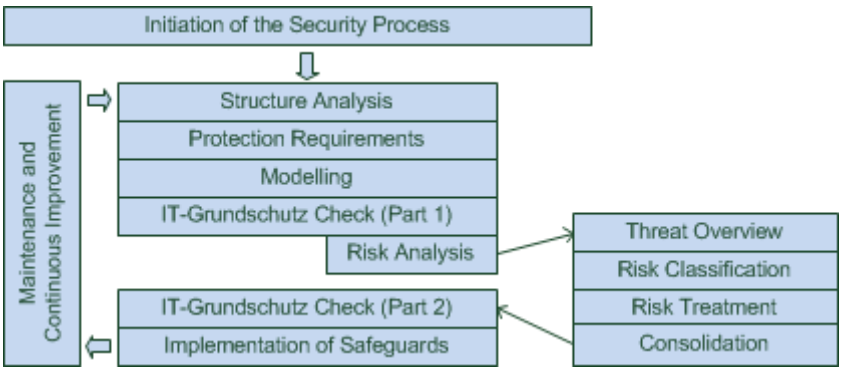


Figure 32: Integration of the risk analysis in the IT-Grundschutz process

The standard can be used when organisations are already working successfully with the IT-Grundschutz Methodology and would like to directly add a risk analysis to the IT-Grundschutz. For this, the BSI-Standard 200-3 *Risk analysis based on IT-Grundschutz* recommends the following additional work steps, which are briefly listed here:

- Establishment of a risk management process
  The risk analysis is an important component of the information security management system (ISMS). The basic prerequisites for this should therefore be specified by the organisation's management. The basic approach of the organisation for performance of risk analyses should be documented in a policy (see BSI-Standard 200-3, Section 2) and passed by the management level.

- Preparing the threat summary
  This work step compiles a list of the correspondingly relevant threats for every target object to be analysed. When determining threats, the BSI uses a two-stage approach. The relevant elementary threats are identified first and, based on them, other possible threats (additional threats) going beyond the elementary threats and resulting from the specific scenario of use are determined. This is performed within the scope of joint brainstorming.

- Classification of risks
  Risk analysis has two stages. Here, for every target object and every threat an assessment is performed assuming that security safeguards have already been implemented or planned. These are usually the security safeguards which have been derived from the basic and standard requirements of the IT-Grundschutz Compendium. The first assessment is followed by a second assessment in which possible security safeguards for handling risks are considered. By means of a before-and-after comparison, the effectiveness of the security safeguards which were used to handle risks can be checked.

- Handling of risks
  Different risk acceptance criteria are possible depending on the risk appetite of an organisation. Risk appetite refers to an organisation's tendency how risks are assessed and dealt with. This tendency results from cultural, internal, external or economic influences. There are the following options for dealing with risks:

  - Risks can be avoided (e.g. by restructuring business processes or the information domain).
  - Risks can be reduced through appropriate security safeguards.
  - Risks can be transferred (e.g. by outsourcing or insurance policies).

Then, an organisation must define risk acceptance criteria and map the handling of the risk on such criteria. In all cases, the management must be involved in the decision how the risks identified are dealt with, because there may be substantial damage or additional costs.

The threat assessment and risk handling steps are performed until the risk acceptance criteria of the organisation have been fulfilled and the remaining risk ("residual risk") is thus in accordance with the organisation's objectives and specifications. The remaining risk must then be submitted to the management level for approval ("**risk acceptance**"). This documents in a traceable manner that the organisation is aware of the residual risk.

- Consolidating the security concept
  The extended security concept must be consolidated before continuing the original IT-Grundschutz process. Here, suitability, interaction, user-friendliness and appropriateness of the security safeguards are checked as a whole.

- In addition, the BSI-Standard 200-3 *Risk analysis based on IT-Grundschutz* explains how the methodology is to be applied if the information domain includes target objects for which the IT-Grundschutz Compendium does not yet contain a suitable module.

A detailed presentation of the methodology can be found in BSI Standard 200-3.

Important: The risk analysis based on IT-Grundschutz is a methodology to determining security safeguards that go beyond the security requirements stated in the IT-Grundschutz Compendium if these are required. Although this methodology has been simplified compared with many other similar approaches, it is often accompanied by considerable cost. In order to remove the most important security problems as quickly as possible, it is sometimes appropriate to *first* fulfil the IT-Grundschutz

requirements in full and only then perform a risk analysis (in contrast to the scheme stated above). Although this means undertaking a few steps repeatedly, the IT-Grundschutz requirements will be fulfilled more quickly. This alternative order is in particular appropriate if

- the information domain under review has already been implemented and is in use, and
- the present target objects can be adequately modelled with the existing IT-Grundschutz Compendium.

For planned information domains or those with atypical technologies or usage scenarios the original order described above is recommended. The following table summarises the advantages and disadvantages of the two alternative orders:

Risk analysis directly after the IT-Grundschutz Check	**Risk analysis after completely implementing the security safeguards**
Potential advantages: • It avoids additional expense, as no security measures that have to be replaced by stronger ones as part of the risk analysis are implemented. • Any essential high-security safeguards are identified and implemented earlier.	Potential advantages: • Security safeguards are implemented earlier as the risk analysis is frequently complicated. • Elementary gaps in security are dealt with first before advanced threats are analysed.
Potential disadvantages: • Security safeguards are implemented later as the risk analysis is frequently complicated. • Elementary gaps in security may be neglected whilst advanced threats are analysed.	Potential disadvantages: • It may incur additional expense, as some security safeguards that have to be replaced by stronger ones as part of the risk analysis may be implemented. • Any essential high-security safeguards are identified and implemented later.

It is also important that a *Risk analysis based on IT-Grundschutz* is frequently easier to perform if it is used subsequently on small sub-elements of the information domain. As a first step, for example, the analysis may be restricted to the geographical, physical infrastructure, i.e. to protection against fire, water and unauthorised access as well as proper power supplies and air conditioning.
Many public agencies and companies already have procedures for risk analysis and/or risk handling being implemented. In such cases it may be reasonable to also apply the present procedures for information security and, if applicable, to only use partial aspects of BSI-Standard 200-3 to ensure uniform methodology. Internationally, a number of different approaches for performance of risk analysis have been established in the area of information security. Such procedures are different e.g. with regard to level of detail, formulation and main topics. Depending on the framework conditions of an organisation and the type of information domain it can be reasonable to use another established approach or an adjusted methodology for analysis of information risks as an alternative to BSI-Standard.

Action points on 8.5 Risk analysis
• Document basic procedure of the organisation for performance of risk analyses in a policy and present this to the management level for passing • Determine the target objects or groups of target objects for which a risk analysis should be performed • Systematically work through BSI-Standard 200-3 *Risk analysis based on IT-Grundschutz*

- Integrate the results of the risk analyses into the security concept

9 Implementation of the security concept

This section presents various aspects that must be considered when planning and implementing security safeguards. It describes how the implementation of security safeguards can be planned, performed, supervised and monitored. There are implementation recommendations for many modules of IT-Grundschutz, including exemplary recommendations for security safeguards for implementing the requirements of the modules. These are based on best practices and long-term experience of experts from the area of information security. However, the safeguards of the implementation recommendations must not be deemed to be mandatory, but they can and should be supplemented or replaced by own safeguards. Such own safeguards again should be notified to the IT-Grundschutz team of BSI, above all if they include new aspects so that the implementation recommendations can be supplemented correspondingly.

When drawing up the security concept, the structure analysis, the definition of the protection needs and the modelling have been performed for the examined information domain. Furthermore, the results of the IT-Grundschutz Check, i.e. of the subsequent gap analysis, are present at such point in time. If any risk analysis has been performed for selected areas, the suggestions for additional safeguards to be implemented which have been put forward as a result should also be available and considered in the process.

There are usually only limited resources in terms of money and personnel available to implement the safeguards. The objective of the steps described in the following is therefore to achieve the most efficient implementation of the intended security safeguards possible. An example to explain the procedure is found at the end of this section.

9.1 Reviewing the results of the study

An overall review should be used to assess the requirements of the IT-Grundschutz modules that have not been implemented or only have been implemented partially. Here, it is recommended to extract them from the results of the IT-Grundschutz Check and to summarise them in a table.

Risk analyses could possibly identify further requirements to be fulfilled as well as safeguards to be implemented. These too should be drawn up in the form of a table. These additional requirements and safeguards should be arranged by subject in line with the target objects examined during modelling and the corresponding IT-Grundschutz modules.

The requirements of the IT-Grundschutz modules to be fulfilled must be specified for security safeguards based on the organisational and technical situation of the organisation. The implementation recommendations of IT-Grundschutz provide practical recommendations for many modules and requirements. Moreover, all the requirements and the correspondingly derived security safeguards should be reviewed again to ensure that they are appropriate: They must provide effective protection for the potential threats and be able to be implemented in practice; they may not, for example, hinder organisational processes or weaken other security measures. Furthermore, they must be economical, see below. In such cases it can become necessary to adjust certain IT-Grundschutz requirements so that the same security objectives will be achieved. Basic requirements are of such a fundamental importance that they cannot be replaced usually.

In order to be able subsequently to understand how the concrete list of safeguards was drawn up and refined, this should be suitably documented.

Further notes on consolidation of the security safeguards are also included in the BSI-Standard 200-3 *Risk analysis based on IT-Grundschutz*.

Examples:

- During a risk analysis it was established that, in addition to the IT-Grundschutz requirements, smart card-supported authentication and local encryption of hard disks must be implemented on

clients used for processing HR data. Such additional requirements should be added in the security concept.

- The security concept of a hospital defines that authentication is required for all IT systems and time-out is performed after ten minutes. The IT-Grundschutz Check reveals that this default value is too general and is not suitable for practical use in this form. Correspondingly, the security concept now differentiates as follows:
  - IT systems in the administration area require re-authentication after 15 minutes of inactivity.
  - In case of IT systems in areas where patient and visitor traffic is present, time-out will be performed after five minutes
  - In case of IT systems in treatment rooms, automatic log-off is deactivated. The employees are ordered to log-off after leaving the rooms.

9.2 Estimating the time and expense

As the budget for implementing security safeguards is always limited in practice, it is necessary to determine how much will need to be invested and how much labour this will entail for each safeguard that is to be implemented. When recording theses costs, you must differentiate between one-time and recurrent investment costs and personnel expenses. At this point it should be mentioned that experience shows that savings on technical or infrastructural security safeguards often result in high ongoing labour costs. The other way round, savings regarding personnel quickly result in ever-growing security deficits.

In this regard it is necessary to ascertain whether all the safeguards initially derived from the requirements can be afforded. If there are safeguards that are not economical, alternative safeguards for fulfilling such requirements should be considered. There are many possible solutions also regarding information security. Often, there are various options for fulfilling requirements by using suitable safeguards. If no appropriate safeguard can be identified, the occurring residual risk as well as the decision must be documented. Usually, basic requirements must always be fulfilled; due to their fundamental nature, accepting any residual risk is not envisaged.

If the estimated resources for costs and personnel are available, usually a decision must be made on how many resources should be used for implementing the security safeguards. Here, it is reasonable to present the results of the security check to the management level. To make those responsible aware of the security issues involved, the security vulnerabilities identified (i.e. security requirements not fulfilled or only insufficiently fulfilled) should be presented in terms of their protection needs. Here, reference can also be made to the specific threats that are stated in the relevant modules. Furthermore, it makes sense to prepare a list of the expected costs and efforts to implement the still required safeguards. Then, a decision regarding the budget should be made.

If it proves to be impossible to provide a sufficient budget for implementing all the missing security safeguards, then the residual risk resulting from failure to implement or delay in implementing certain measures should be pointed out. To assist in this, the cross-reference tables from the IT-Grundschutz additional materials can be used. The cross-reference tables provide a summary for each module to identify the requirements that act against certain fundamental threats. Similarly, these tables also can be used to determine the fundamental threats without sufficient protection if requirements of the modules are not fulfilled. The residual risk relating to any chance or wilful threats should be described clearly and presented to the management level for a decision. The remaining steps can only occur after the management level has decided that the residual risk is acceptable, as the management level must bear the responsibility for the consequences.

9.3 Specifying the order of implementation of the safeguards

Section 8.3.3 describes an order for implementation of the modules – from basic and comprehensive modules to such modules covering more specific topics, correspondingly being able to be considered with lower priority regarding time. This order of implementation of the modules is particularly

important when implementing the Basic Protection. It can also be used generally for specifying the order of implementation of the individual safeguards of a security concept.

Basically, the safeguards derived from the basic requirements must be implemented at first, followed by the standard requirements. The additional safeguards for increased protection needs should only be adapted and implemented subsequently.

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

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

- The order of implementation can be based on the point in time when the corresponding safeguards must be implemented within the life cycle of a target object. For example, in case of new target objects, safeguards from the areas of planning and designing should be implemented with higher priority than safeguards regarding secure operation; however, in case of target objects being present in the information domain for a longer period already, the focus should be on safeguarding the operation.
- For some safeguards, there are dependences and logical relationships that require a specific chronological order. Restrictive assignment of rights (basic requirements) on a new server can only be performed if such server has been installed securely (standard requirement). At first sight, such order may collide with the classification of basic and standard requirements. However, basic requirements always have priority as far as they can be fulfilled already, e.g. with an existing server in the above example.
- Some safeguards have a wide-ranging effect and others a restricted, local one. It often makes sense to first handle those safeguards having a wide-ranging effect. This is also a reason for preferentially implementing the basic requirements as they enable the quickest possible safeguarding with a wide-ranging effect. However, it is also worth weighing the safeguards from the various areas on the basis of how quickly they can be implemented and what benefit they have for security. Often, quick wins can be found in the organisational area or can be achieved by central configuration settings.
- Some modules have a larger impact on the desired security level than others. Security measures from such modules should have preference, especially if they remove vulnerabilities in areas that are in need of high protection. Thus, servers should be secured first (e.g. by implementing the module SYS.1.1 *General servers*) and only then the clients connected to them.
- Modules that have many requirements not implemented represent areas with a large number of vulnerabilities. They should also be given preference.

The decision on which security safeguards to undertake or initially delay and where residual risks can be accepted should be documented carefully for legal reasons. In case of doubt, additional opinions should be surveyed and these opinions should be documented as well to prove the duty to take good care was fulfilled in case of a legal battle later on.

Note:

Already in the beginning it has been stated that fulfilling requirements may fail due to lack of resources. The aspects stated above allow for first prioritisation. However, such procedure does not consider the remaining residual risks sufficiently. If requirements of IT-Grundschutz modules are not fulfilled, it is recommended to consider the incurred deficits within the scope of a simplified risk analysis. In such case the determination of threats to be performed in a risk analysis can be omitted. This has been made already when drawing up the IT-Grundschutz modules. Thus, there is still assessment of risks due to the lack of implementation of requirements.

9.4 Specifying the tasks and the responsibility

After determining the order for implementing the safeguards, it must be defined who will implement which and by when. Experience has shown that the implementation will be delayed significantly or skipped completely without such mandatory specifications. In this case, it must be ensured that the person named responsible has the skill and authority necessary to implement the safeguards and that he/she is provided with the necessary resources.

Likewise, it must also be specified who is responsible for monitoring the implementation and who is to be reported of the completion of the implementation of each safeguard. The ISO is usually informed of the completion. The ISO must be notified continuously on advancement of implementation as well as on the results of the implementation. In turn, the ISO must notify the management level regularly on the advancement and the relevant reduction of present risks.

The implementation plan should contain the following information at a minimum:

- description of the target object as operational environment,
- number and/or title of the considered module,
- title and/or description of the requirement to be fulfilled,
- description of the safeguard to be implemented and/or reference to the description in the security concept,
- implementation scheduling, budget planning, e.g. for provisioning and operating costs of components,
- persons responsible for implementation of the safeguards.

9.5 Safeguards accompanying implementation

It is particularly important to identify and/or design the safeguards accompanying the implementation in advance and to include them when planning the implementation of the safeguards. Such safeguards particularly include awareness-raising activities aiming at explaining the issues of information security and to inform the employees being affected by new security safeguards on the necessity and the consequences of the safeguards.

The staff concerned must also receive training as to how to implement and apply the new security safeguards correctly. If such training is not performed, often the safeguards cannot be implemented and will lose their effect if the employees consider themselves as being informed sufficiently, frequently resulting in a negative attitude towards information security.

Example: RECPLAST GmbH

The above steps are described in extracts using the fictional company RECPLAST GmbH as an example. The following table shows some safeguards to be implemented, including the relevant budget planning.

A.6 Implementation Plan for RECPLAST GmbH						
Target Object	**Module**	**Requirement**	**Safeguard**	**Target Date**	**Budget**	**Responsible**
S008 - Print Server	SYS.1.1 General Server	SYS.1.1.A3 Restrictive granting of access rights	A few remaining group rights must be corrected.	Q3 this year	- €	Herr Schmidt (IT Services)
S008 - Print Server	SYS.1.1 General Server	SYS.1.1.A4 Separation of roles	Not every administrator role has a separate user account yet.	31.07. this year	- €	Herr Schmidt (IT Services)
S008 - Print Server	SYS.1.1 General Server	SYS.1.1.A8 Regular data backups	The internal tape backup system should be switched to an external backup. Currently backup solutions are tested.	Q1 next year	Purchase: 15000 Euro, operations: tbd	Frau Lang (Purchasing Dep.)

Figure 33: Implementation plan of RECPLAST GmbH (excerpt)

This information can be used to monitor and control implementation of the safeguards.

Action points on 9 Implementation of the security concept

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

10 Maintenance and continuous improvement of information security

To enable the maintenance and continuous improvement of the information security process, you not only need to implement appropriate security safeguards and update documents continuously, but also need to test the IS process itself regularly in terms of its effectiveness and efficiency. In this case, regular checking of success and evaluations of the IS process must be performed by the management level (management evaluation). If required (e.g. if a number of security incidents occur or there are serious changes to the framework conditions) meetings must be held between the regular ones. All results and decisions must be documented so that the decision can be understood later. The documents must be meaningful and understandable for the corresponding target group, see also Section 5.2 *Information flow within information security process*. The task of the ISO is to collect and process such information and to correspondingly edit them for the management level in a brief and clear manner.

10.1 Checking the information security process at all levels

Checking the information security process is essential as, on the one hand, this will detect and remove errors and weaknesses and, on the other, the efficiency of the IS process can be further improved. Amongst others, the objective is to improve the practical nature of the strategy, safeguards and organisational processes. The key aspects that have to be considered are shown below.

To check and improve the efficiency of the information security process, procedures and mechanisms should be established that check the implementation of the safeguards agreed, on the one hand, and their effectiveness and efficiency, on the other.

Thus, the information security strategy should also make key statements on measuring the achievement of objectives; here, at least the following should be defined:

- which objectives are monitored or measured in which form and reasonable number (WHAT)
- who is responsible for monitoring or measuring the items specified before (WHO)
- when and how often are the results to be evaluated (WHEN)

Basically, checking the information security process should be limited to a reasonable number of objectives. Examples of methods may include:

- Definition, documentation and assessment of key figures (e.g. up-to-datedness of anti-virus protection and number of detected malware programmes, etc.)
- Detecting, documenting and assessing security incidents
- Performance of exercises and tests for simulation of security incidents and documentation of results (e.g. restoring a back-up)
- Internal and external audits, data protection checks
- Certification in accordance with specified security criteria (e.g. ISO 27001 on the basis of IT-Grundschutz:)

Successful implementation of security safeguards should be checked regularly. Basically, it is important that checks and audits are not performed by the persons having developed the respective security specifications and that management of the organisation is informed on the state of information security based on the results of the audit.

For avoidance of blind spots it may be appropriate to instruct external experts to perform such auditing activities.

Since the cost of audits varies with the complexity and size of the information domain, the requirements can be well implemented even by small organisations. Automated monitoring and

reporting can be used to enable continuous analysis of information security with low impact on the resources. In case of small organisations, reviewing of available documentations for checking up-to-datedness as well as a workshop for discussing problems and experience with the security concept may provide already a sufficient summary of the state of information security.

10.1.1 Checking by using key figures

In information security, key figures are used to make the IS process or partial aspects of such process measurable. They are used for optimising the process and checking quality, efficiency and effectiveness of the present security safeguards.

Frequently, measurements and key figures are used for communication with the management and may provide valuable argumentation aids for the information security management. Thus, it is important to select measurement tools and edit performed measurements in such a way so that they fit into the strategic environment of the own organisation.

Determining key figures always means efforts. Such efforts should be reasonably related to the desired and/or achieved results. Key figures also have a limited significance as they highlight single, in most cases only a few areas of information security, i.e. such areas where measurements can be made easily. This generally applies to technical security where sensors can be used to automatically state measurement values and other statements that can be quantified easily, such as

- number of detected malware patterns
- number of installed security patches
- duration of system failures
- number of performed security trainings

Key figures always can be interpreted differently; thus, it is important to clarify in advance the objective of the measurements and how and with which efforts this should be achieved. Then, measuring against such objective can be performed.

10.1.2 Assessing the ISMS using a maturity model

The effectiveness of the management system for information security of an organisation should be assessed regularly. This can be performed by using a maturity model. A maturity model makes it possible to understandably document the advancement of the ISMS during the years without providing too much details on individual safeguards. It represents another potential key figure for controlling the information security in an organisation. An exemplary maturity assessment of an ISMS can be as follows:

Maturity level	Explanation
0	There is no ISMS and there are no plans for establishing an ISMS.
1	An ISMS is planned, but not established.
2	An ISMS is partially established.
3	An ISMS is fully established and documented.
4	In addition to maturity level 3, the ISMS is checked regularly for effectiveness.
5	In addition to maturity level 4, the ISMS is improved regularly.

Assessment of the maturity level of an ISMS can be multi-dimensional based on topics, e.g. based on the layer model of IT-Grundschutz:

- ISMS *(Information Security Management Systems)*
- ORP *(Organisation and Planning)*
- CON *(Concepts)*
- OPS *(Operation)*
- DER *(Detection and Reaction)*
- INF *(Infrastructure)*
- NET *(Networks and Communication)*
- SYS *(IT Systems)*
- APP *(Applications)*
- IND *(Industrial IT)*

Information security is a cross-sectional function that is connected to almost all areas of an organisation. That is why it is necessary to integrate the information security into the existing processes of an organisation. Examples of this include:

- Project management: The protection needs of the information to be processed as results later on must be assessed and suitable security safeguards based on this must be planned during the planning phase of a project already.
- Incident management: In case of failures of the IT operations having an impact on information security, the procedure must be coordinated with the security management. The security incident management and the fault management of the IT and the facility managements must be connected to each other.

If such management processes do not exist, it will be possible to draw up and operate an ISMS, but this will not work efficiently. If the ISMS is not connected to the project management, the protection needs of new or changed business processes can only be determined by cyclic queries (annually, quarterly). This makes it much harder to obtain a complete and up-to-date definition of the protection needs of all target objects. If no fault management is present, security incidents will not be detected and/or not reported to the correct body. Thus, the maturity level of information security also depends on the maturity level of the other management processes of the organisation and is not an independent value.

The maturity level of the information security can be different amongst organisations. The sole fact that security management is present cannot be the basis for concluding that the organisation will be able to manage security incidents in a good manner. Uniform and differentiated assessment of the level of implementation of the ISMS of an organisation may achieve various important targets:

- Checking whether the individual aspects of the security management have been processed and implemented completely.
- Detecting potentials for improvement and further development.
- Comparability of the level of implementation of security management between various organisations.
- Verifiability of the achieved implementation level regarding third parties.

In addition, the management level may also use the assessment results as key figures for controlling and further developing the security management system (see Section 5.2.1).

If the implementation level is evaluated regularly, the continuous further development of the information security management of the organisation can be documented in an understandable and efficient manner.

10.1.3 Checking implementation of the security safeguards

The implementation plan includes the persons and deadlines for implementation of all safeguards of the security concept (list of tasks and time schedule). This allows for evaluating how such planning is complied with. Checking the information security processes serves for controlling the activities within the scope of the security concept and for identifying planning errors.

After introduction of new security safeguards, the ISO should check whether the employees are exhibiting adequate acceptance. The causes of lack of acceptance must be discovered and eliminated.

Security audit

The information security audit (IS audit) is a part of every successful information security management. Only regular checking of the established security safeguards and of the information security process may enable statements on their effective implementation, up-to-datedness, completeness and appropriateness and correspondingly also on the current state of the information security. Thus, the IS audit is a tool for determining, achieving and maintaining an appropriate security level in an organisation. For this, BSI provides the *Guide for IS revision on the basis of IT-Grundschutz* for developing a procedure to determine the status of the information security and to identify vulnerabilities (see [BSIR]).

The security requirements included in the IT-Grundschutz Compendium can also be used to perform an audit of information security. For this, it is recommended to pursue the same approach used for the IT-Grundschutz Check. Producing a separate check-list for each module of the IT-Grundschutz Compendium based on the requirements, which is adapted to the organisation, is helpful and reduces the workload. This facilitates the performance of audits and improves the reproducibility of the results.

Cyber security check

By means of implementing a cyber security check, organisations can determine the current cyber security level of their organisation. The cyber security check is intended for organisations that have not been dealing extensively with the topic of cyber security so far. Performing a cyber security check explicitly does not impose any mandatory prerequisites regarding situation of the documents or implementation status (see [CSC]).

The cyber security check and the underlying safeguard objectives for the assessment of cyber security were designed in such a manner that the risk of falling victim to a cyber attack can be minimised by regularly implementing a cyber security check. In this respect, the approach focuses on cyber security issues and aspects.

The BSI and the ISACA provide practical action guidelines containing specific guidelines and information for the implementation of a cyber security check and for the preparation of the report. Making an assignment of the safeguard objectives to be assessed to the known standards of information security available (IT-Grundschutz, ISO 27001, COBIT, PCI DSS) is a particularly interesting added value.

10.1.4 ISO 27001 certification on the basis of IT-Grundschutz

A certification is a method for having checked the achievement of security objectives and implementation of the security safeguards by qualified independent bodies. ISO 27001 certification based on IT-Grundschutz provides understandable, repeatable and comparable audit results to an organisation.

10.2 Suitability of information security strategy

In order to be able to successfully control and manage the information security process, the management level must understand the extent to which security objectives can actually be achieved with the aid of the security strategy used.

Up-to-datedness of security objectives, framework conditions and security concept

From a longer term perspective it is necessary to check the security objectives set and the framework conditions. In particular in rapidly changing industries, appropriate alterations in the security policy and strategy are of essential importance.

Operational (e.g. use of new IT systems, moves) and organisational changes (e.g. outsourcing) and changes of legal requirements must be incorporated into the security concept as early as the planning phase. The security concept and the related documentation must be updated with each relevant change. This must also be incorporated into the organisation's change process. Therefore, the information security process must be integrated into the organisation's change management.

Examination of cost-effectiveness

Cost-effectiveness of the security strategy and the specific security measures should be monitored constantly. It should be checked whether the actually incurred costs correspond to the originally planned costs, or whether other alternative security safeguards being more favourable regarding the resources can be used. It is also important to regularly state the benefits of the existing security measures.

Feedback from internals and externals

Generally, feedback on errors and vulnerabilities in the processes does not only originate from the information security organisations or auditing, but also from employees, business partners, customers or partners. Thus, the organisation must establish an effective approach for handling complaints and other feedback from internals and externals. Complaints by customers or employees can also be an indicator for dissatisfaction. Emerging dissatisfaction should be counteracted as much as possible because satisfied employees show a lower risk of negligent or intentional actions possibly disturbing operation.

Thus, there must be a clearly defined procedure and explicitly specified competences for handling complaints and for feedback on problems to the responsible body. A response to complaints should be provided as fast as possible so that the person filing the complaint feels to be taken seriously. The reported problems must be assessed and the need for action must be estimated. The organisation must implement appropriate corrective actions for removing the causes of errors in order to prevent them from occurring again.

Further development of ISMS

The ISMS must be further developed continuously and adapted to recent knowledge e.g. resulting from checking the information security process.

Extension of selected approach

When entering the security process, the management of the organisation must decide on a approach to achieve a certain security level for a defined scope of application on the basis of IT-Grundschutz or other methods. After implementing such approach and achieving the phase of maintenance and continuous improvement of the information security, it should be considered whether

- the chosen approach should be supplemented (e.g. from Basic Protection to Standard Protection) and/or
- the scope of application should be extended (e.g. from Core Protection of a limited area to a larger information domain).

The objective should be to raise all areas of the organisation to a holistic security level at last including Standard Protection on the long term.

10.3 Taking over the results into the information security process

The results of the assessment are required for improving the IS process. It may be possible that the security objectives, the security strategy or the security concept needs to be changed and the security organisation should be adapted to the requirements. It may be appropriate to change business processes, processes or the IT environment, e.g. if security objectives cannot be achieved under the

previous framework conditions or only with difficulty (i.e. at great financial and staffing expense). If large-scale changes are made or comprehensive changes are implemented, the management circle closes and the planning phase starts again.

Checks on the individual topics must be performed by appropriate persons who have the required skills and independence. The person who produced the concepts should not undertake completion or plausibility checks. Performed improvements, corrections and adjustments should be documented.

The basic approach of the organisation for checking and improving the information security process should be documented in a corresponding policy and should be passed by the management level. The **policy for checking and improving the information security level** particularly should stipulate how internal audits in the area of information security should be performed, and how the results are included into the change process. Test results and reports are generally to be considered as confidential and must therefore be protected particularly well.

Action points on 10 Maintenance and continuous improvement of information security

- Document basic approach of the organisation for checking and improving the information security process in a corresponding policy and present this to the management level for passing
- Integrate measurement of the achievement of objectives into the security strategy
- Check adherence to implementation plan
- Check implementation of the safeguards agreed
- Check the effectiveness and efficiency of the safeguards agreed
- Check whether the security safeguards have been accepted and improve if necessary
- Consider conflict of roles between creator and auditor
- Ensure confidentiality of the examination results
- Check suitability and up-to-datedness of security objectives, strategies and concept
- Check appropriateness of resources provided and the cost-effectiveness of the security strategy and security safeguards
- Allow results of checks to flow into improvements in the information security process

11 ISO 27001 certification on the basis of IT-Grundschutz

The company or public agency may obtain certification according to ISO/IEC 27001 to show successful implementation of IT-Grundschutz. The BSI developed a certification scheme for information security considering the requirements on management systems for information security according to ISO/IEC 27001 and uses the IT-Grundschutz Compendium as well as the BSI-Standards 200-x as check-lists. That is why this is termed ISO 27001 certification on the basis of IT-Grundschutz. Such certification is intended for Standard Protection and basically possible for Core Protection. In case of pure Basic Protection, the implemented security safeguards will not be sufficient for certification, but they can be used as entry for one of the two other approaches.

The ISO 27001 certificate on the basis of IT-Grundschutz provides companies and public agencies with the option of making its efforts for information security transparent to others. This may act as a quality feature to both customers and business partners and therefore result in a competitive advantage.

Here, the interest in an ISO 27001 certification on the basis of IT-Grundschutz is diverse:

- Service providers see in such a certificate a reliable way of demonstrating that they have implemented the IT-Grundschutz safeguards.
- Partner companies are interested in knowing what degree of information security their business partners are able to provide.
- Organisations that newly link up to a network are asked to provide evidence that information security in their organisations is sufficient to rule out the possibility of any unacceptable risks resulting from these organisations being connected to the network.
- Organisations are interested in providing evidence to customers/the public of the effort they put into achieving an adequate level of information security.

As the IT-Grundschutz, including the approach for security management as described in this document and the security requirements included in the IT-Grundschutz Compendium, has not become a quasi-standard for information security, it would be reasonable to use this as generally acknowledged set of criteria of information security.

The basis for obtaining an ISO 27001 certificate on the basis of IT-Grundschutz is an audit performed by an external auditor certified by BSI. The audit produces an audit report that is presented to the certification body, which will decide on awarding the ISO 27001 certificate on the basis of IT-Grundschutz. Sets of criteria of the approach include the ISO 27001 standard and the IT-Grundschutz approach described in this document as well as the IT-Grundschutz Compendium of the BSI.

An ISO 27001 certificate on the basis of IT-Grundschutz demonstrates that IT-Grundschutz has been implemented successfully in the considered information domain. In addition, such certificate also demonstrates that the organisation

- recognises the importance of information security,
- has a functioning IS management system, and also
- has achieved a defined level of security at a particular point in time.

Further information on certification in accordance with ISO 27001 and on certification as ISO 27001 auditor on the basis of IT-Grundschutz are included in the web offer of the BSI (see [ZERT]).

Action points on 11 ISO 27001 certification on the basis of IT-Grundschutz

- Read information on the scheme for ISO 27001 certification on the basis of IT-Grundschutz
- Check whether work regarding information security should be made transparent by means of an ISO 27001 certificate on the basis of IT-Grundschutz

- If necessary, check whether the information security management and the security status meet the relevant requirements.
- If necessary, initiate the certification process

12 Appendix

12.1 Explanations for the damage scenarios

The following states exemplary questions for the damage scenarios defined in Section 8.2.1. These questions should serve as an aid for defining the protection needs, above all in the area of applications. The questions should be adapted and supplemented on the basis of the individual requirements.

Damage scenario "Violation of laws, regulations or contracts"

Such violations can result from the loss of confidentiality, integrity or availability. The severity of the ensuing damage will often depend on the specific legal implications for this organisation.

Examples of relevant German legislation are:

> The Constitution, the Civil Code, the Penal Code, the Federal Data Protection Act and the data protection legislation of the individual States, the General Data Protection Regulation of the EU (GDPR [GDPR]), the Social Security Code, the Commercial Code, the Staff Representation Act, the Employees' Representation 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 security measuring business/industrial secrets.

Questions:

Loss of confidentiality

- Is confidentiality of the information required by law?
- Is disclosure of information likely to result in criminal prosecution or a claim for compensation?
- Are contracts involved that include the maintenance of the confidentiality of certain information?

Loss of integrity

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

Loss of availability

- Would failure of the application result in violation of any regulations or even of laws?
- Is certain information required to be available at all times by law?
- Have any deadlines been set which must be observed when using the application?
- Are there any contractual conditions for certain deadlines which have to be observed?

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

When implementing and operating IT systems and applications there is a risk of violating informational self-determination or even 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 data processing or the transmission of personal data,
- unauthorised disclosure of personal data,
- use of personal data for a purpose other than the permitted one for which it was collected, and
- corruption of personal data in IT systems or during the transmission of data.

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

Questions:

Loss of confidentiality

- What harm could come to an individual if 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 is provided, for example, on the person's health or economic situation?
- What loss or damage could be caused by misuse of stored personal data?

Loss of integrity

- What harm could come to an individual if personal data were to be corrupted by accident or wilfully tampered with?
- When would the loss of integrity of personal data first be noticed?

Loss of availability

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

Damage scenario "Physical injury"

The malfunctioning of IT systems or applications can result directly in injury, disability or even death of persons. The extent of the damage must be assessed on the basis of the direct personal damage.

Examples of such applications and IT systems are:

- medical monitoring computers,
- medical diagnosis systems,
- flight control computers, and
- traffic routing systems.

Questions:

Loss of confidentiality

- Could a person be physically or psychologically injured through the disclosure of information?

Loss of integrity

- Could tampering with programme sequences or data endanger people's health?

Loss of availability

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

Damage scenario "Impaired performance of duties"

In particular the loss of availability of an application or the loss of integrity of information or data can substantially affect the ability of an organisation to fulfil its tasks. In this context, the severity of any ensuing damage depends on the duration of the impairment and the extent to which the services offered are constrained.

Examples of this include:

- non-adherence to deadlines due to delays in the handling of administrative procedures,
- late delivery due to delayed processing of orders,
- faulty production due to incorrect control parameters, and
- insufficient quality assurance due to the failure of a test system.

Questions:

Loss of confidentiality

- Is there any information whose confidentiality is critical to task performance (e.g. criminal prosecution information, investigation findings)?

Loss of integrity

- Could alteration of information restrict the performance of tasks such that the organisation will be unable to act?
- Would significant damage be caused if tasks were performed using corrupt information? When would unauthorised data alterations be detected at the earliest?
- Could corrupted information data in the application under review lead to errors in other applications?
- If data was incorrectly attributed to a person who did not actually generate it, what would be the consequences?

Loss of availability

- Is there information for which limitation of availability would have serious consequences on the organisation or its business processes?
- Can the failure of applications so severely affect the operation of an organisation that the waiting times for those affected are not longer acceptable?
- Would any other applications be affected by the failure of this application?
- Is it important to the organisation that access to applications, including programmes and data, must be ensured at all times?

Damage scenario "Negative internal or external effects"

Various negative internal and external effects can be produced by the loss of one of the three basic values – confidentiality, integrity or availability - for example:

- loss of reputation of an organisation,
- loss of confidence regarding an organisation,
- loss of employee morale,
- impairment of commercial relations between partner organisations,
- loss of confidence in the quality of an organisation's work, and

- loss of competitive position.

The level of damage depends on the severity of the loss in trust or level of dissemination of the internal or external effect.

Such damage can have a variety of causes:

- an organisation's inability to act due to IT system failure,
- incorrect publications because of manipulated data,
- wrong placing of orders due to faulty stock control programmes,
- non-compliance with confidentiality agreements,
- blame assigned to the wrong people,
- one department is unable perform its duties due to errors in other areas,
- passing on of “wanted list” data to interested third parties, and
- leaking of confidential data to the press.

Questions:

Loss of confidentiality

- What implications would the unauthorised publication of sensitive information have for the organisation?
- Can the loss of confidentiality of information result in a weaker competitive position?
- Would the disclosure of confidential information raise doubts about the trustworthiness of the organisation?
- Could the publication of information lead to political or social insecurity?
- Can employees lose their confidence in the organisation as a result of unauthorised publication of information?

Loss of integrity

- What damage could result from the processing, dissemination or transmission of incorrect or incomplete information?
- Would the information corruption become publicly known?
- Could the publication of corrupted information lead to a loss of prestige?
- Could the publication of corrupted information lead to political or social insecurity?
- Could corrupted information lead to reduced product quality and thus to loss of prestige?

Loss of availability

- Would the failure of applications restrict information services provided to external parties?
- Does the non-availability of information or the failure of business processes prevent the organisation from achieving its business objectives?
- When is the non-availability of information or the failure of applications or business processes noted externally?

Damage scenario “Financial consequences”

Direct or indirect financial damage can occur through the loss of confidentiality to data requiring protection, changes to information or the failure of applications. Examples include:

- unauthorised release of R&D results,
- manipulation of financially-relevant data in an accounting system,
- failure of an IT-controlled production system, resulting in a drop in sales,
- unauthorised obtaining knowledge of marketing strategy papers or of turnover 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 overall level of damage is comprised of the costs that are incurred directly or indirectly, for example through damage to property, claims for damage and additional costs (e.g. for restoration).

Questions:

Loss of confidentiality

- Could the publication of confidential information result in claims for compensation?
- Are there information with business processes or applications that could provide financial advantage if accessed by third parties (e.g. competitors)?
- Is any research data of significant value stored using applications? What would happen if such data was copied and passed on without permission?
- Could any damage be caused by premature publication of sensitive information?

Loss of integrity

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

Loss of availability

- Would failure of applications or business processes impair production, inventory management or distribution?
- If applications or business processes fail, would there be financial losses due to delayed payments or lost interest?
- How much would it cost to repair or restore IT systems if it were to fail, develop a fault, be destroyed or stolen?
- Could the failure of applications or business processes result in an inability to pay or contractual penalty?
- How many important customers would be affected by the failure of applications or business processes?

12.2 References

[27000] ISO/IEC 27000:2016 "Information technology - Security techniques – Information Security management systems - Overview and vocabulary", ISO/IEC JTC 1/SC 27

[27001] ISO/IEC 27001:2013 "Information technology - Security techniques - Information security management systems - Requirements", ISO/IEC JTC 1/SC 27

[27002] ISO/IEC 27002:2013 "Information technology - Security techniques - Code of practice for information security controls", ISO/IEC JTC 1/SC 27

[27004] ISO/IEC 27004:2016 “Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation“, ISO/IECJTC 1/SC 27

[27005] ISO/IEC 27005:2011 "Information technology - Security techniques - Information security risk management", ISO/IEC JTC 1/SC 27

[820-2] DIN 820-2:2012, Annex H, Presentation of documents - Verbal forms for the expression of provisions, NA 173-00-02 AA

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

[BSI3] Risk analysis based on IT-Grundschutz, BSI-Standard 200-3, https://www.bsi.bund.de/grundschutz

[BSIR] Information security revision - A guide for IS revision on the basis of IT-Grundschutz, BSI, Version 2.0, March 2010, https://www.bsi.bund.de/

[CSC] Cyber Security Check guideline, BSI, ISACA, 07 March 2014, https://www.allianz-fuer-cybersicherheit.de

[GDPR] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 27 April 2016, European Parliament and Council of the European Union

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

[ISF] The Standard of Good Practice 2016, ISF - Information Security Forum, 2016

[NIST53] NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, NIST, 2015, http://csrc.nist.gov/publications/PubsSPs.html

[RFC2119] RFC 2119 (Key words for use in RFCs to Indicate Requirement Levels), Network Working Group, Stand 1997, https://www.ietf.org/rfc/rfc2119.txt

[SDM] Standard data protection model (SDM), SDM-Methodik-Handbuch, V1.0, Conference of the Federal and State Data Protection Officers, can be downloaded from all web servers of the German regulatory data protection authorities, e.g https://www.datenschutz-mv.de/datenschutz/sdm/sdm.html

[ZERT] Information on certification in accordance with ISO 27001 on the basis of IT-Grundschutz, BSI, https://www.bsi.bund.de/iso27001-zertifikate