Federal Office
for Information Security

IT-Grundschutz Online Course

Print version

Last update: 07.08.2018

Change History

This document contains the print version of the online course IT-Grundschutz

Version	Datum	Name	Beschreibung
0.9	06.06.2018	Fraunhofer SIT	Final draft
1.0	07.08.2018	Fraunhofer SIT	Final version

Federal Office for Information Security
P.O.B. 20 03 63
D-53133 Bonn (Germany)
Phone: +49 (0) 22899 9582-5369
E-mail: grundschutz@bsi.bund.de
Website: https://www.bsi.bund.de

Table of Contents

List of Illustrations

List of Tables

Lesson 1: Introduction

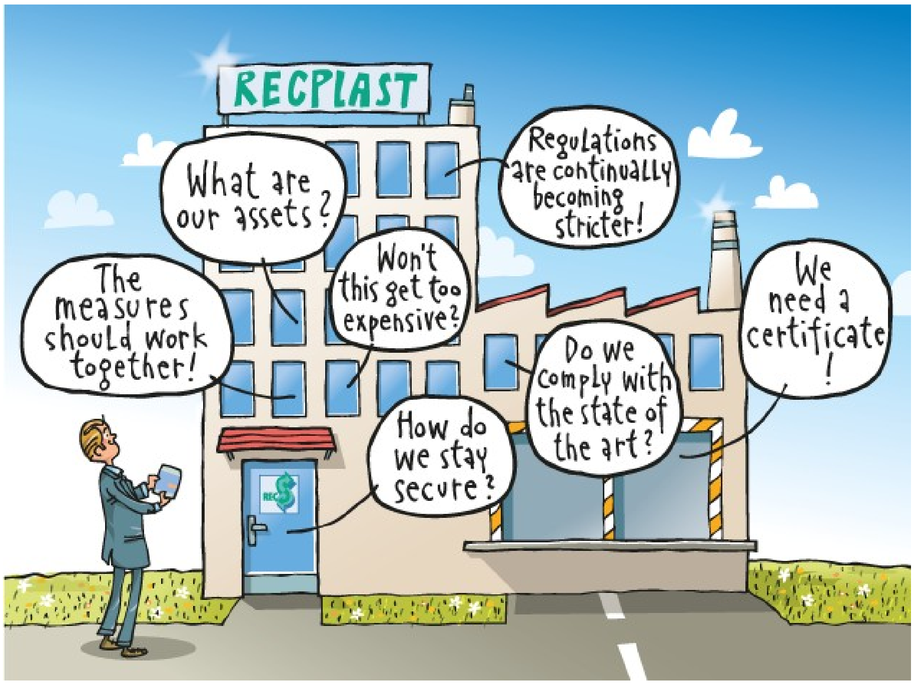
For today's companies and public authorities, ensuring that **information** is accurate and treated as confidential when necessary is essential. This means it is equally important that the **technical systems** in which information is stored, processed, or transmitted function seamlessly and are **effectively protected against a diverse array of constantly evolving threats**.

- Would you like to know whether the information security measures you have taken are sufficient to prevent severe losses and respond appropriately to related incidents?
- Do you need assistance in developing a security concept?
- Are you looking for support in conducting a systematic review of the security measures planned or already in place in your area of responsibility?
- Do you want these measures to meet generally recognised standards?

If you answered “yes” to any of these questions, you should take a look at **IT-Grundschutz**. These guidelines describe in detail the **requirements** that need to be fulfilled to achieve a level of security appropriate for the demands of typical areas of application (and easily extensible when increased security is needed) in a cost-efficient manner. They also present a widely recognised **methodology** that can show you efficient ways to develop and verify a security concept that is tailored to the characteristics of your facilities.

While there are many paths to information security, IT-Grundschutz gives you an efficient means of achieving this goal while keeping an eye on potential threats and avoiding detours along the way. To put it in visual terms, **IT-Grundschutz is not just a road map, but a full-fledged guide to information security!**

Unit 1.1: Why IT-Grundschutz?


RECPLAST
What are our assets?
Regulations are continually becoming stricter!
The measures should work together!
Won't this get too expensive?
We need a certificate!
Do we comply with the state of the art?
How do we stay secure?

Information security needs to be able to cope with **a variety of challenges**:

- **Threat complexity:** Threats can stem from a wide array of causes and hinder the aims of information security in many different ways. Cyber attacks, negligence, and technical flaws require just as much attention as natural disasters and other forms of force majeure.
- **All-encompassing security concepts:** Information security requires measures on multiple levels. These include not just the IT systems at hand, but organisational aspects, personnel, physical infrastructure, workplaces, and operational processes, as well.
- **Integration of security measures**: To ensure that the security measures in place are sufficiently able to deal with complex threats, the corresponding organisational, technical, and infrastructural protections must be suitable for the organisation in question; aligned with the threats it actually faces in practice; integrated in sensible ways; and both well-understood and supported by the organisation's administrators and employees.
- **Appropriateness of security measures**: The efficiency and appropriateness of security measures must also be taken into account. While it is important to take effective measures against present threats, these measures should also reflect the actual level of protection needed and not demand too much of the organisation in question. Efforts that are inordinately expensive are to be avoided, as are precautions that place undue strain on an organisation's key processes.
- **Compliance with external requirements**: Today, many companies and public authorities are facing an ever increasing need to prove that they have taken adequate steps to ensure information security. Rendering such proof is easier when an organisation aligns its information security measures with generally recognised standards.
- **Sustainability of security measures**: Finally, security is not something one achieves once and never has to worry about again. Just as companies and public authorities themselves evolve, so do the information, processes, and goods they work with that are deserving of protection. By the same token, new types of vulnerabilities and threats make it necessary to review and enhance established security concepts.

The **BSI's IT-Grundschutz guidelines** offer a solid basis for meeting these challenges in a professional manner and structuring corresponding information security measures. They are designed to provide companies and public authorities with a systematic means of searching for weaknesses, reviewing the appropriateness of the protective measures they have implemented, and developing and updating security concepts that both reflect the business processes, specialised tasks, and organisational structures of their respective organisations and fulfil generally recognised standards.

Unit 1.2: IT-Grundschutz – Components

The BSI's IT-Grundschutz guidelines consist of a series of individual components. At their core, they comprise the following:

- The **BSI Standards for Information Security**, which include recommendations on organisational frameworks and methods for ensuring information security
- The **IT-Grundschutz Compendium**, which can be used to translate the general recommendations formulated in the BSI Standards into concrete actions.

In this course, you will learn more about these publications and the specific assistance they can offer you in ensuring information security at your own organisation. The next section presents some basic information on how these and other IT-Grundschutz documents and resources are organised.

The BSI Standards for Information Security

Unternehmen und Wirtschaft

Bundesamt für Sicherheit in der Informationstechnik

Informationssicherheit und IT-Grundschutz

BSI-Standards 200-1, 200-2 und 200-3

3. Auflage

Bundesanzeiger Verlag

BSI Standard 200-1: *Information Security Management Systems (ISMS)* describes the essential requirements an information security management system must fulfil, the components it must contain, and the tasks it must perform. These requirements are presented in a manner that reflects the specifications of the ISO 27001 norm and other international standards of information security.

BSI Standard 200-2: *IT-Grundschutz Methodology* provides methodological support for the step-by-step implementation of an ISMS at a given organisation and describes efficient ways to turn the general requirements of BSI Standard 200-1 and the underlying ISO/IEC 27001 norm into specific actions.

BSI Standard 200-3: *Risk Analysis Based on IT-Grundschutz* describes an approach to analysing risk that is simpler than other methods. This approach is helpful and important when components need to be secured, but there is uncertainty as to whether fulfilling the basic and standard requirements at hand will provide for adequate security.

The IT-Grundschutz Compendium

Unternehmen und Wirtschaft

Bundesamt für Sicherheit in der Informationstechnik

IT-Grundschutz-Kompendium

Standardwerk zur Informationssicherheit

Bundesanzeiger Verlag

The IT-Grundschutz Compendium is an extensive, modularly structured **tool and reference for the topic of information security**. It consists of the **IT-Grundschutz modules**, which are arranged in 10 thematic layers and explore their own different aspects.

Each module begins with a brief introduction, followed by a statement of its objectives and an explanation of how its subject matter differs from that of the other modules. After presenting a general description of the specific threats at hand, each module covers the security requirements that are relevant to its subject.

The greatest advantage you gain in using the IT-Grundschutz Compendium is that in most cases involving normal protection requirements, you no longer having to carry out complex risk analyses in the situations described in these modules. Seasoned security experts have already done this work, and the BSI has incorporated it into its security requirements.

The requirements presented in the modules describe **what** should be done to ensure an appropriate level of security. **How** this can and should be handled is covered in the supplementary **implementation recommendations** that the BSI publishes for most modules.

Further publications and resources

The BSI also offers other documents, tools, and resources that are designed to help attain an adequate level of security. These include the **IT-Grundschutz profiles**, which are model solutions that companies and public authorities can use as templates for developing their own security concepts in specific areas of application. In addition, **ISO 27001 certification based on IT-Grundschutz** provides organisations with a means of proving that their technical and organisational measures in the area of information security correspond to recognised standards.

The **BSI's webpages** on **IT-Grundschutz** contain all the relevant information on these and other useful offerings. Electronic versions of the BSI Standards and the IT-Grundschutz Compendium are also provided, along with tips on how to obtain printed version of these documents.

An array of **software tools** from various providers are also available to support the IT-Grundschutz methodology. The use of one of these tools is not only helpful, but advisable for organisations of a certain size and larger. An overview and further recommendations on the information provided by the BSI are available here.

If you would like to engage in a **professional dialogue on IT-Grundschutz** and meet other users and organisations interested in this subject, you may be interested in the corresponding XING group. All the **latest news** related to IT-Grundschutz can also be found on Twitter. If you wish to stay up-to-date on IT-Grundschutz, you can subscribe to the BSI's **IT-Grundschutz newsletter**, as well.

Unit 1.3: About this course

When it comes to the holistic implementation of information security, different organisations have different prerequisites and starting points. Small and midsize organisations, for example, often lack the personnel and financial resources to secure all their areas in a single step. This is why they may find it more practical to start by concentrating on implementing fundamental security measures or safeguarding specific areas that are in particular need of protection. The **IT-Grundschutz methodology** described in BSI Standard 200-2 thus includes **three variants** a given organisation can choose from to achieve a level of security suitable for its requirements and situation:

- The **Basic Protection** offers an easy way to get started in systematic information security management by showing how an organisation can significantly improve its security by meeting some crucial basic prerequisites. They involve no differentiated assessments of the level of protection required or supplementary risk analyses. If you would like to learn more about how this works, the Guide to Basic Protection Based on IT-Grundschutz: Information Security in Three Steps offers a compact, clearly organised starting point to an approach that should be of particular interest to small and midsize companies and public authorities.
- With the help of the **Standard Protection**, an organisation can achieve comprehensive protection by starting with a systematic inventory of the various components its security concept needs to take into account. These measures also involve assessing one's security requirements using the IT-Grundschutz Compendium and, in isolated cases, conducting additional risk analyses that prove necessary.

- Finally, the **Core Protection** includes all the steps involved in the Standard Protection, but focus on select areas of particular importance (the “crown jewels”, so to speak) within the organisation at hand.

Structure

Before choosing and following one of these approaches, an organisation must have established a certain organisational foundation. In this course, you will find out more about the attendant aspects in

Lesson 1: *Security management*.

The lessons thereafter will then provide in-depth information about the individual **steps involved in implementing the Standard Protection** in accordance with IT-Grundschutz.

- Lesson 2: *Structure analysis*,
- Lesson 3: *Determining protection requirements*,
- Lesson 4: *Modelling in Accordance with IT-Grundschutz*,
- Lesson 5: *IT-Grundschutz Check*,
- Lesson 6: *Risk analysis,*
- Lesson 7: *Implementation planning*.

Rather than a finish line to cross, security is an ongoing process in which decisions taken and measures put in place must be reviewed in terms of their appropriateness and efficacy on a regular basis and adapted to new circumstances as required. In the final Lesson 8: *Maintenance and improvement*, you will learn about procedures you can follow to ensure a solid level of security for the long term at your organisation. It will also tell you more about **ISO 27001 certification based on IT-Grundschutz.Grundschutz**.

The example company RECPLAST GmbH

The individual steps of the IT-Grundschutz methodology are illustrated throughout this course with the help of an example: the fictional company RECPLAST GmbH, which is also used in the BSI standards. In both those standards and this course, you will be presented with excerpts from the results documents of various phases of the IT-Grundschutz methodology. A more comprehensive account is available in a separate PDF document.

About the pictograms used

In this course, the following pictograms are used to highlight certain passages of text:

Exclamation points are used to point out key phrases, recommendations, and text that is important for other reasons.

References to further detailed or supplementary information in the essential IT-Grundschutz documents or other sources are indicated by a book symbol.

This symbol is used to mark questions and exercises with which you can test what you have just learned about IT-Grundschutz.

This symbol indicates sections that deal with RECPLAST GmbH, the fictional company used as an example throughout this course.

Linguistic note

For the sake of readability, this document does not include both the male and female variants of certain formulations. Any such formulations should be understood as referring to both genders.

Lesson 1: Security management

We need a holistic concept for an ISMS!
Why? Our security technology is perfect!

These days, every organisation needs a security apparatus to shield it from the dangers of the Internet. This almost always includes antivirus programmes and spam filters, and often more complex solutions such as multiple firewalls and threat recognition software, as well. Companies and public authorities also take organisational measures – for example, by establishing guidelines for the use of mobile systems or making their employees aware of online hazards. In many cases, however, such technologies are used and organisational measures are implemented without a corresponding concept or efforts to track their success.

Experience has shown that taking individual technical or organisational measures in isolation is neither efficient nor effective as a means of ensuring adequate information security. It is much more important to establish a framework in which all such efforts can be controlled and monitored in a goal-oriented fashion. An **information security management system (ISMS)** of this kind consists of four components:

- **Management principles**,
  such as in setting organisational goals, establishing communication policies, and creating rules for cost-benefit analyses
- **Resources and employees**,
  which involves managing the use of technology and personnel
- A description of a **security process**

But what should you keep in mind when assembling an operating an ISMS?

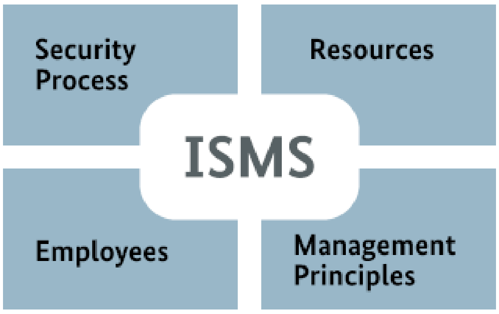


Illustration 1: Components of a ISMS

To find out, please refer to BSI Standard 200-1: *Information Security Management Systems (ISMS)*. The recommendations provided therein are described in terms of specific actions to take in BSI Standard 200-2: *IT-Grundschutz Methodology*. Chapters 3 and 4 of this standard include insights into the aspects that require particular attention when initiating and organising a security process.

In this lesson, you will learn about the essential aspects of information security management in accordance with IT-Grundschutz.

- How should a security process be designed?
- What are the fundamental management principles?
- How is a solid security organisation structured?
- How is a security policy formulated?
- What are the basic steps involved in establishing a security concept?
- What are the characteristics of good documentation?

Unit 1.4: The Security Process

Information security is not a finish line one has to cross once, but a process that requires continuous adjustment. Changes in an organisation's procedures, shifting conditions in the surrounding legal framework, new technologies, and previously unknown vulnerabilities (along with the risks they present) give rise to new requirements on a regular basis, which means that long-term appropriateness and efficacy are not automatically guaranteed. The overall **security process is thus subject to a life cycle** that comprises the following phases:

- **Plan** – planning security measures
- **Do** – implementing the measures
- **Check** – tracking success and the achievement of objectives
- **Act** – eliminating flaws and making improvements

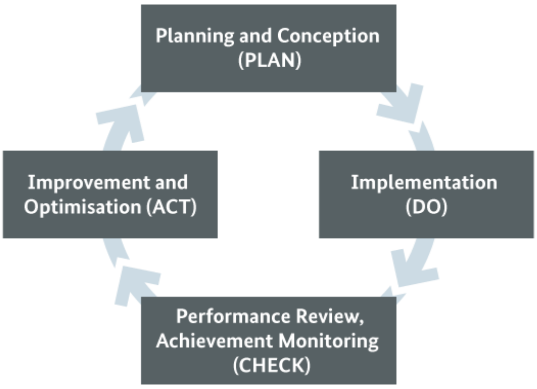

Planning and Conception (PLAN)
Implementation (DO)
Performance Review, Achievement Monitoring (CHECK)
Improvement and Optimisation (ACT)

Illustration 2: The PDCA-Cycle

The **PDCA cycle**, a concept created by William Edwards Deming, is a proven component of many management systems (in quality and environmental management, for example).

Success tracking and continuous improvement are particularly important as management principles in the security process. Without regular inspection, it is impossible to guarantee the long-term efficacy of organisational and technical safeguards.

Rather than fulfilling some inherent purpose, **good documentation** provides for transparency in designing the security process and taking related decisions, which helps avoid misunderstandings. It does not have to be available on paper. In fact, electronic documentation offers the advantage of being easy to update and quickly accessible when needed, although it is important to be diligent in implementing corresponding access privileges.

In order to protect information appropriately, its importance to the organisation at hand must be clear. **Classifying information** according to its degree of confidentiality and establishing corresponding rules on how it is to be handled can be helpful in this regard. Classification labels, for example, give every employee a direct means of identifying how information is to be treated.

For more important notes on the requirements documentation should fulfil and the design of information flows and reporting lines in the security process, please refer to chapter five of BSI Standard 200-2: *IT-Grundschutz Methodology*. The beginning of the chapter includes a description of a procedural model for classifying information.

Unit 1.5: Phases of the Security Process

For an orderly security process to be established, a given organisation's top administrators must initiate the process, set related objectives and framework conditions, assemble an organisational structure, and make the necessary resources available.

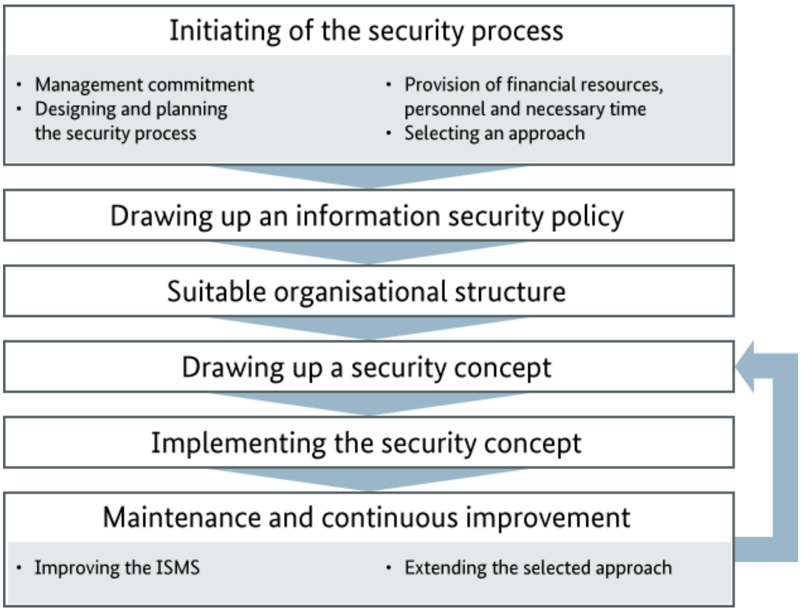

Initiating of the security process
• Management commitment
• Designing and planning the security process
• Provision of financial resources, personnel and necessary time
• Selecting an approach
Drawing up an information security policy
Suitable organisational structure
Drawing up a security concept
Implementing the security concept
Maintenance and continuous improvement
• Improving the ISMS
• Extending the selected approach

Illustration 3: Phases of the security process

The security process consists of the individual phases and sub-activities presented below.

1. Initiating and creating an information security policy, assembling a security organisation

To ensure that your security process corresponds to your organisation's particular needs, the first step is to identify and analyse the relevant **framework conditions**. These include the security requirements customers expect you to meet and those formulated by the authorities as legal obligations. If regulatory obligations are in play, they will have a strong influence on your security objectives and the concepts you need to develop. To the extent that your organisation has already started information security initiatives, they must be identified and evaluated; if technical and organisational measures have already been implemented, they need to be integrated into the process you plan to design.

As mentioned above, the objectives associated with your security process will have a profound impact on its design. **Information security objectives** are derived from an organisation's goals and the surrounding circumstances in which it operates. They are incorporated into an **information security policy** and brought to the attention of all the organisation's employees. These objectives also serve as a basis for deriving the level of security you need your business processes to uphold.

To implement the necessary measures, you then need to assemble a **security organisation** and define corresponding responsibilities. **Additional resources** such as offices, funding, and time must also be provided.

Finally, information security is a task to be handled not just by executives and security organisation teams, but by **all employees within their respective purviews**. Without their cooperation, an organisation will fail to achieve its security objectives.

2. Creating a security concept

In order to achieve your security objectives, you will need to define suitable **technical and organisational measures** in an overarching concept. These can include:

- Measures to ensure the physical security of buildings and other premises
- Technical mechanisms to secure the interfaces of a given network and its individual segments
- Rules on how classified information must be handled
- An appropriate system of identity and authorisation management
- The use of cryptographic measures
- Sufficient data backup procedures
- Procedures to identify and thwart malware

The subsequent lessons in this course will describe the process of designing security concepts in detail in accordance with IT-Grundschutz.

3. Implementing the concept

A security concept must describe how the measures it contains are to be implemented and reviewed. This enables the executives at a given organisation to evaluate the actions taken.

4. Maintenance and improvement

Instead of a project with a defined end point, information security is an ongoing process in which you adapt your security concept to evolving requirements. Here, suitable instruments (key figures and internal and external audits, for example) must be used to regularly check whether your information security objectives are being fulfilled. Improvements need to be made to address any deviations from these goals.

Unit 1.6: Executive Tasks and Responsibilities

Whether an organisation succeeds in implementing a solid ISMS and making ongoing improvements to it depends largely on how its top management level perceives its related tasks and responsibilities. Executives' most important obligations include:

- Knowing the risks involved in information security violations, establishing a corresponding framework, and taking fundamental decisions on how such risks are to be addressed
- Initiating, managing, and monitoring the security process and ensuring that information security is integrated into all of their organisation's processes and projects
- Providing the resources necessary for security management (personnel, budget, time) while factoring in corresponding costs and benefits
- Setting an example by demonstrating a commitment to security

An institution's top management level bears the **overall responsibility** for the adequacy of its ISMS. Delegating operational responsibilities and encouraging employees to be aware of security concerns during their work does not change this fact.

Are your organisation's executives prepared to take on the tasks and responsibilities listed above? If not, an essential prerequisite of information security has not been met. Module ISMS.1 *Security management* of the IT-Grundschutz Compendium presents the resulting risks and describes the requirements that need to be fulfilled to address them.

Unit 1.7: Information Security Officers

To facilitate the clear assignment of responsibilities for operational tasks, an information security officer (ISO) needs to be appointed.

Responsibilities and tasks

An information security officer is responsible for all issues related to information security at his or her organisation. His or her tasks include:

- Controlling and coordinating the security process
- Supporting management in creating an IT security policy
- Coordinating the creation of a security concept, along with its sub-concepts and guidelines
- Preparing plans for the implementation of security measures, initiating said implementation, and conducting corresponding reviews
- Reporting to management and other individuals responsible for security on the organisation's current information security status
- coordinating projects relating to security,
- Investigating security-related incidents
- Initiating and coordinating training courses and other measures designed to raise awareness of information security

An ISO should have experience and expertise in areas of both information security and IT in general. He or she should also be familiar with the business processes of the organisation at hand.

To **ensure his or her independence**, an ISO should be directly assigned to the organisation's top management level. Integrating an ISO into an IT department can lead to role conflicts, as he or she may not be able to fulfil certain obligations in monitoring security measures without outside influence. Allowing the same person to serve as information security officer and data protection officer can also lead to problems. In such situations, the lines dividing these two roles must be clearly defined to prevent conflicts.

In addition, an ISO needs sufficient **time and resources to undergo the necessary ongoing training**. He or she must **report directly to the executive level** to facilitate prompt decisions when conflicts arise.

Depending on the size of the company or government agency in question, **multiple ISOs** may be needed for the organisation's different areas, locations, or large-scale projects.

For further information on the profile an ISO should fulfil, please refer to chapter 4.4 of BSI Standard 200-2: *IT-Grundschutz Methodology*. The implementation recommendations for module ISMS.1 also include important notes on an ISO's tasks and qualification profile (in ISMS.1.M4).

Unit 1.8: Information Security Officers for ICS

In many areas, the security requirements in industrial production differ from those pertaining to office IT. Planning, implementing, and monitoring security measures that are appropriate for industrial control systems (ICS) requires a great deal of specific knowledge of these systems and what is necessary in operating them. It thus makes sense for manufacturing companies to appoint an **ICS information security officer (ICS-ISO)** with sufficient related experience. He or she should be integrated into a company's security organisation and cooperate closely with the ISO.

An **ICS-ISO's essential tasks** include the following:

- Pursuing shared objectives pertaining to both industrial control and the company's overall ISMS while providing active project support
- Implementing general security requirements and guidelines in the field of ICS
- Carrying out risk analyses in the field of ICS
- Establishing and carrying out security measures in the field of ICS
- Creating security guidelines and concepts for ICS while factoring in functional safety requirements and conducting employee training
- Serving as a point of contact for on-site employees and the organisation as a whole
- Designing courses and other measures to raise awareness
- Addressing security incidents along with the ISO
- Maintaining documentation

For further information on the profile an ICS-ISO should fulfil, please refer to chapter 4.7 of BSI Standard 200-2: IT-Grundschutz Methodology.

Unit 1.9: The IS Management Team

At larger organisations, a team of multiple members responsible for information security should be formed to support the information security officer. This team should be responsible for coordinating and handling all overarching concerns related to information security, as well as for providing guidance and monitoring corresponding analyses, concepts, and guidelines.

Within this **IS management team**, the ISO, the ICS-ISO (if applicable), IT managers, those responsible for data protection, and representatives assigned to particular technical procedures and business processes should work together. In relevant cases, they should also be supported by further ISOs that have been appointed for specific areas, projects, or IT systems (in the same manner as an ICS-ISO). The following figure depicts how an organisational structure might look:

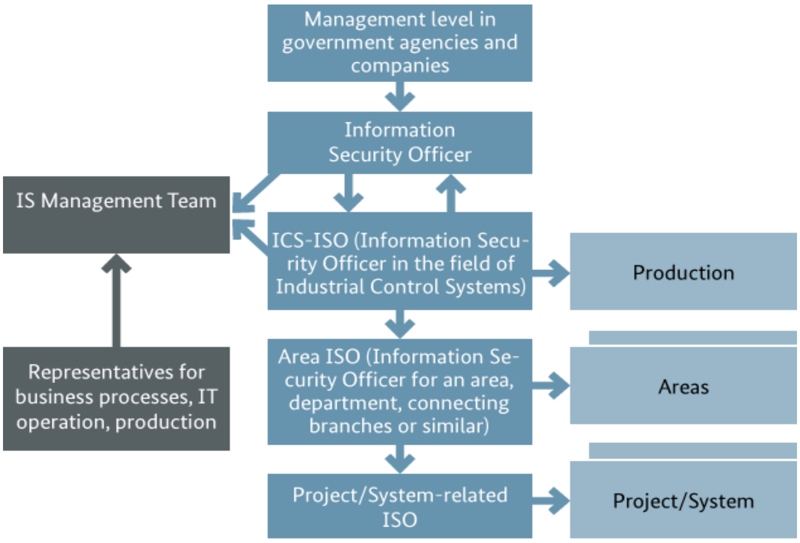

Management level in government agencies and companies
Information Security Officer
IS Management Team
ICS-ISO (Information Security Officer in the field of Industrial Control Systems)
Production
Representatives for business processes, IT operation, production
Area ISO (Information Security Officer for an area, department, connecting branches or similar)
Areas
Project/System-related ISO
Project/System

Illustration 4: Organisation of information security roles

An **IS management team's tasks** include:

- Establishing security objectives and strategies and developing an information security policy
- Reviewing the implementation of the security policy
- Initiating, directing, and monitoring the security process
- Helping to draw up a security concept
- Checking whether the security measures planned in the concept are suitable, effective, and working as intended
- Designing training and awareness programmes for information security
- Providing guidance to those responsible for specialised areas and IT operations, the ISO in specified areas (if applicable), the ICS-ISO, and the top management level

Whether or not it makes sense to assemble an IS management team or appoint multiple ISOs to areas or projects depends on the size of the organisation at hand. At smaller organisations, a single ISO with the necessary expertise is typically sufficient.

For models of security organisation structures at small, midsize, and larger organisations and explanations of the tasks assigned to ISOs, ICS-ISOs, and IS management teams, please refer to chapter 4 *(Organisation of the Security Process)* of BSI Standard 200-2: *IT-Grundschutz Methodology* and module ISMS.1 *Security management* of the IT-Grundschutz Compendium.

Example of how a company's security organisation can be structured

The executives at our example company, RECPLAST GmbH, want to have a mandatory **security concept** developed for the entire organisation. To this end, the company needs to define its established information security principles and guidelines in a more precise manner.

RECPLAST thus starts by appointing an **information security officer**, who will be responsible for coordinating its related efforts. Since this position will require extensive IT expertise, the company chooses an employee from its information technology department; in connection with these new tasks, the employee will, however, report to the executive board. The board also appoints an **ICS information security officer**, who will be tasked with developing and monitoring security requirements and measures in production. After that, the company initiates a security concept project that is to produce the following results by a certain deadline:

1. Proposals and decision support regarding an information security policy
2. A security concept proposal and a corresponding implementation plan
3. Proposed measures to maintain information security
4. Documentation on all decision support, decisions taken, and measures implemented in connection with the information security process

Since the ISO does not have detailed knowledge of the company’s business processes, an **IS management team** is formed to aid the ISO and the ICS-ISO in creating a security policy and concept. The team includes the company's data protection officer, the head of its business division and legal department, and a sales employee (to take customer requirements into account). This means every business area is represented, and the team can obtain further information on operational procedures and external demands when necessary.

The project is then presented to RECPLAST's works council, which will receive regular reports on the interim results achieved. Its employees are also informed of the project and its objectives at a company meeting.

Application exercise

Could this example be applied to your company or government agency?

- Does your organisation have an ISO? If so, how was this person appointed and what area does he or she typically work in?
- How does the ISO fit into your organisation's hierarchy?
- Do you have an IS management team? If so, who are its members?
- Assuming your organisation has a production area, does it also have an ICS-ISO? If so, how does he or she collaborate with your ISO?

Please compare the regulations in place at your organisation with those at the example company RECPLAST and those described in BSI Standard 200-2: *IT-Grundschutz Methodology*. Where do you see differences? What is your assessment of them? Do you think your organisation needs to improve?

Unit 1.10: Security Policy

An information security policy is an **essential executive document** that defines the priority information security has at a given organisation, along with binding principles and the level of security the organisation wishes to achieve. In just a few pages, it should describe the organisation's security objectives and the organisational framework in which they are to be achieved in a manner the employees affected can understand. The development of this policy must be initiated and actively supported by the organisation's executives. The ISO will be responsible for creating the policy in close cooperation with said executives with the assistance of the IS management team (if one exists) and other individuals responsible for information security.

The policy must be **brought to the attention of all affected employees** and **updated on an ongoing basis**.

What should be established in an information security policy?

- The scope should be specified.
- The policy should highlight how important information security is to the organisation at hand – by pointing out, for example, how IT failures or violations of the confidentiality or integrity of information can threaten the organisation's existence.
- The responsibility borne by the organisation's executives should be emphasised in terms of both the initiation of the security process and its ongoing improvement.
- The policy should reference the applicable laws and regulatory requirements and the employees' obligation to observe them.
- The business processes that are particularly important with regard to information security (such as production workflows, research procedures, and personnel processing) should be specified, along with the importance of strict compliance with security regulations.
- The policy should present an organisational structure for information security and the tasks of the various individuals responsible for security.
- It is also helpful to reference security training courses and measures designed to raise related awareness.

The module ISMS.1 Security management describes the requirements a security policy should fulfil. The corresponding implementation recommendations contain tips on the structure of this subject and how to proceed.

Example: the information security policy at RECPLAST GmbH

RECPLAST GmbH has developed its own security policy. It addresses the following topics:

- The importance of the policy and information security in general
- The company's objectives and desired level of security
- Responsibilities,
- Violations and corresponding consequences
- The scope and how the policy applies in practice
- This example can be found in chapter 2 of the in-depth presentation of RECPLAST GmbH.

Application exercise

Please take a moment to consider how you would design a security policy for your company or government agency.

- How would you define its scope?
- What objectives would you set?
- Does your organisation already have officers assigned to information security or individual aspects of this area? If so, how would you involve them in the development process?
- How would you present the tasks and responsibilities of the employees at your organisation?
- Are there any especially critical business processes with requirements you would want to emphasise in the policy?

Unit 1.11: Security Concepts

The measures with which the objectives and strategies laid out in an **information security policy** are to be pursued are described in a corresponding security concept. A security concept of this kind always has a defined scope. In the IT-Grundschutz methodology, this is referred to as an **information network**.

Defining an information network

An information network must have a **sensible minimum size**. To achieve comprehensive security, it is generally advisable to examine the entire organisation in question. That said, it is often more practical – particularly at larger organisations and when security measures have thus far been taken on more of a case-by-case basis rather than in line with a systematic concept – to concentrate (initially) on **specific areas**. These should, however,

- be **easy to delineate** based on their organisational structures or applications and
- include **essential tasks and business processes** of the organisation under review.

Viable sub-areas may include one or more organisational units, business processes, or specialised tasks. Individual clients, servers, or network connections, on the other hand, are not suitable for examination.

When defining an information network, make sure to describe its interfaces in specific detail. This is particularly important when the business processes or specialised tasks involved depend on services provided by external partners.

Initial inventory of an information network

In the initial phase of the security process, it is not necessary to describe applications or IT infrastructure in detail. At first, the focus should be more on characterising crucial business processes within the scope of the concept in terms of their informationsecurity requirements. It is enough to know which processes have normal, high, or very high security requirements.

This then serves as a basis for taking an **initial inventory of the information network**. Here, the following information and details must be compiled in a structured (e.g. tabular) format:

- Business processes within the information network (name, description, entity responsible)
- Applications involved in these processes (name, description)
- IT systems and ICS components (name, system platform, place of installation (if applicable))
- Facilities important to the information network, such as a data centre or server rooms (type, room number, building)
- Virtual systems (identified and labelled accordingly)

A graphical network diagram can be a helpful complement to a tabular overview of IT systems.

The components identified, along with the information network as a whole, constitute **target objects** of the security concept. Prior to the actual development of this concept, you should have a rough idea of the levels of protection required by the different target objects you identified in the initial inventory.

Choosing an Approach

Before fleshing out the details of your findings thus far, you will need to choose an approach. Here, the IT-Grundschutz methodology provides for **three variants** an organisation can choose from depending on its own particular situation. These variants differ with regard to the breadth and depth of the safeguards to be implemented:

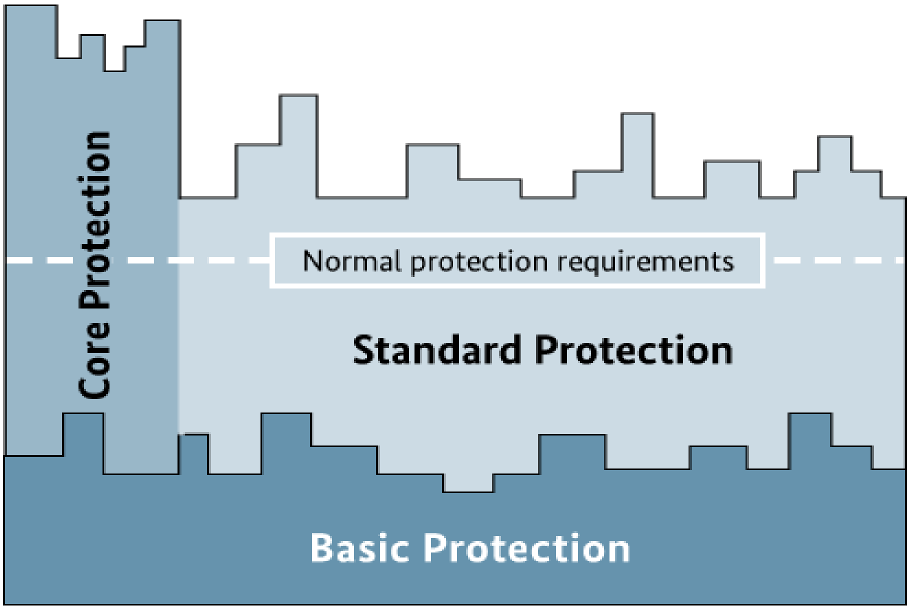
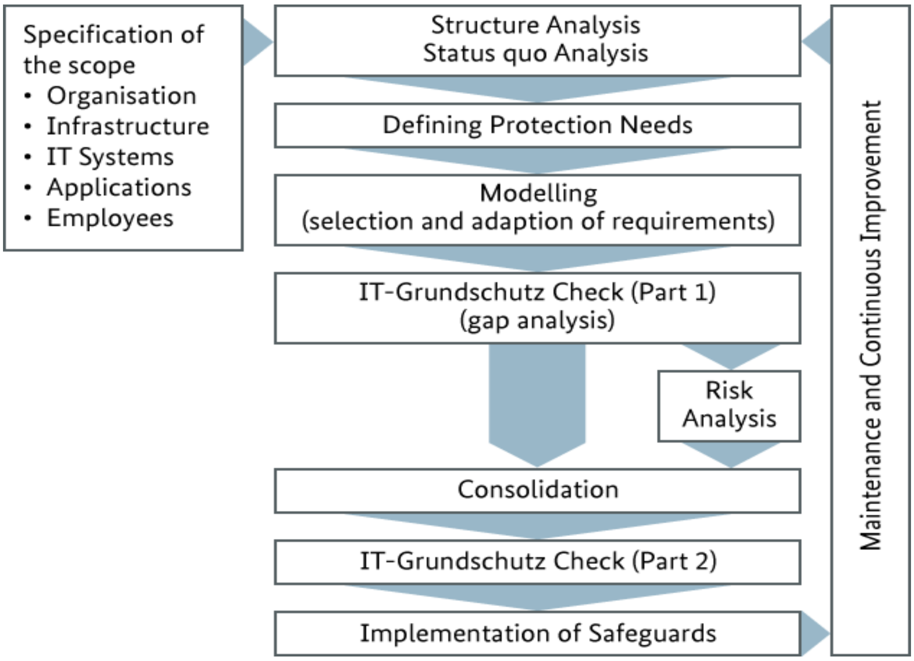


Illustration 5: Variants of the IT-Grundschutz methodology

- The **Basic Protection** should be of interest to organisations that are looking to get started with IT-Grundschutz and quickly secure all their relevant business processes on a basic level.
- The Core Protection focuses on the security of an organisation's "crown jewels" – that is, its crucial business processes and *assets*. In other words, this variant seeks to achieve in-depth protection of the most critical areas.
- The Standard Protection correspond to the recommended IT-Grundschutz approach (comparable to the previous BSI Standard 100-2).
- Their aim is to implement comprehensive protection of all the processes and areas at an organisation.

Both the basic and the Core Protection can serve as an entry point to achieving comprehensive security in line with IT-Grundschutz.

This course describes the approach to implementing the Standard Protection and references the other two variants when appropriate. The following illustration depicts the steps involved:


Specification of the scope
• Organisation
• Infrastructure
• IT Systems
• Applications
• Employees
Structure Analysis
Status quo Analysis
Defining Protection Needs
Modelling
(selection and adaption of requirements)
IT-Grundschutz Check (Part 1)
(gap analysis)
Risk Analysis
Consolidation
IT-Grundschutz Check (Part 2)
Implementation of Safeguards
Maintenance and Continuous Improvement

Illlustration 6: Steps involved in implementing the standard safeguards of the IT-Grundschutz methodology

The three variants of the IT-Grundschutz methodology are presented in detail in chapters 6, 7, and 8 of BSI Standard 200-2. The Basic Protection is also covered extensively in a separate guide based on IT-Grundschutz. Implementation recommendations are available in ISMS1.M10: Drawing *a security concept*, as well.

Unit 1.12: Test questions

If you wish, you can use the following questions to test your knowledge of information security management. See the attachment for solutions to the questions.
Please note that multiple answers may be correct.

1 **Which model is based on the security process described in BSI Standard 200-1?**

a A cycle comprising four steps: plan, do, check, and act

b A method of defining a state-of-the-art information security level

c A model designed to facilitate continuous improvement

d A model consisting of technical security safeguards

2 **Was should an information security policy contain?**

a Detailed technical requirements for configuring important IT systems

b Statements on the importance of information security for the organisation in question

c Fundamental rules on organising information security

d Specific rules on how confidential information is to be handled

3 **For which tasks is an information security officer typically responsible?**

a Coordinating the development of security concepts

b Configuring the security technology in use

c Reporting to management on the current information security status

d answer questions from the media related to the status of information security in companies

4 **What is an appropriate way to build an IS management team?**

a Each department of a company or government agency sends employees, ensuring that all areas are covered.

b The IT manager alone appoints several employees to the team.

c The composition is on a volunteer basis. Anyone who is interested will be included.

d Management assembles the team from those responsible for certain IT systems, applications, data protection, IT service and (if available) ICS-ISB.

5 **Who is responsible for approving the information security policy?**

a The IS management team

b ISB

c The executives at the company or government agency at hand

d PR department in a company or government agency

6 **Why could it be useful to decide on a security concept in accordance with Basic Protection?**

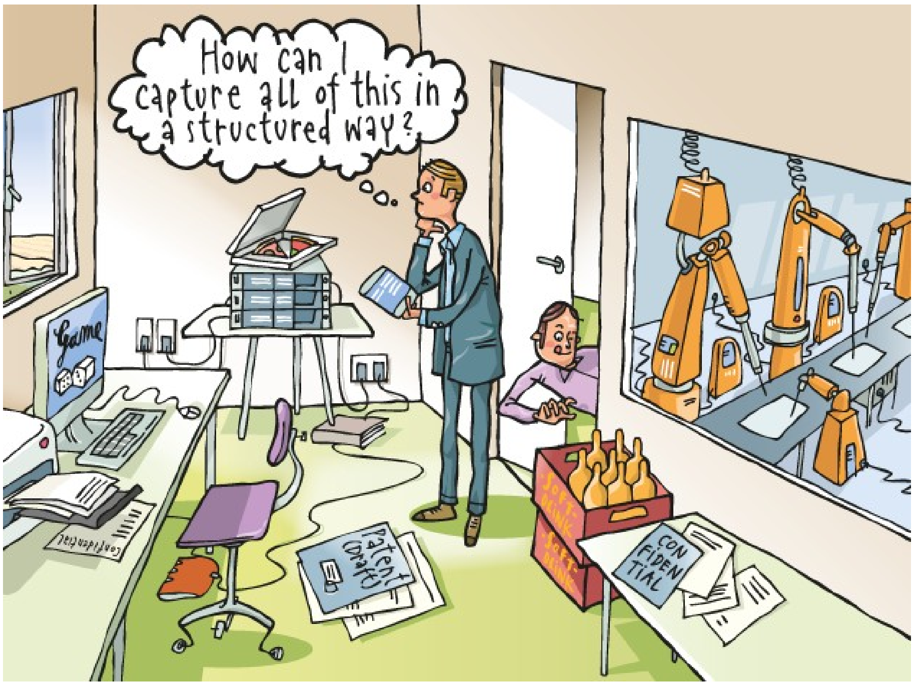
a Meeting the associated requirements is entirely sufficient for a normal company in most cases.

b The organisation in question needs to achieve information security in short order and the Basic Protection presents a suitable entry point.

c The organisation in question wants to achieve information security incrementally. In the medium term, the security concept in accordance with standard security can be expanded.

d There is an urgent need to protect valuable information The Basic Protection provides for suitable protection of an organisation's “crown jewels”

Lesson 2: Structure analysis



What are the key tasks and business processes of companies, government agencies, and other organisations? What information is required, processed, or stored in these processes and tasks? What applications are used, and in what infrastructural environment does this take place? What IT systems are involved?

The more accurately you can answer these questions for the information network at hand, the more you will be able to target the individual protective measures in your security concept. The **aim of structural analysis** is to assemble and refine the knowledge this process requires. In performing structural analysis, you will round out the results of the initial inventory you took of your processes, applications, and IT systems (see Unit 1.11: *Security Concepts*).

In this lesson, RECPLAST GmbH will be used as an example to show you which detailed information you will need to collect through structural analysis for the different components of your information network.

- How can you document **business processes, applications,** and the key **information** used therein?
- How should a **network diagram** be configured, and what information should it include?
- What information is required on the various types of **IT systems** running (or planned for use) in the information network in question?
- How can you take the **spatial circumstances** at hand (properties, buildings, rooms, production sites) into account?

Unit 2.1: The Example Company RECPLAST GmbH

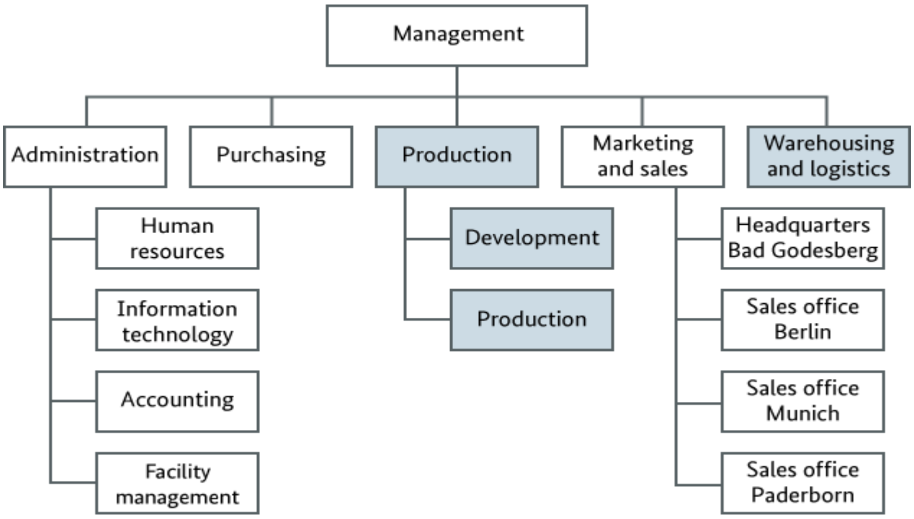
Like the other steps in implementing the Standard Protection of the IT-Grundschutz methodology, this lesson explains structural analysis using RECPLAST GmbH as an example. Here is some advance introductory information on this fictional company.

Business purpose and locations

RECPLAST GmbH employs around 500 people and produces some 400 different plastic products using recyclable materials. Its administrative, production, and warehouse facilities are located in Bonn, Germany, but in different parts of the city: Its executive and administrative offices, along with its purchasing and sales and marketing departments, recently moved into a new building in Bad Godesberg, while its development, production, material storage, and distribution facilities have remained at the company's original headquarters in Beuel. RECPLAST also has sales offices in Berlin, Munich, and Paderborn.

Organisational structure

The following organisational chart illustrates how the company is structured. The departments displayed on a grey background are based in Bonn-Beuel; all the others (except for the sales offices) are located at RECPLAST’s administrative headquarters in Bad Godesberg.

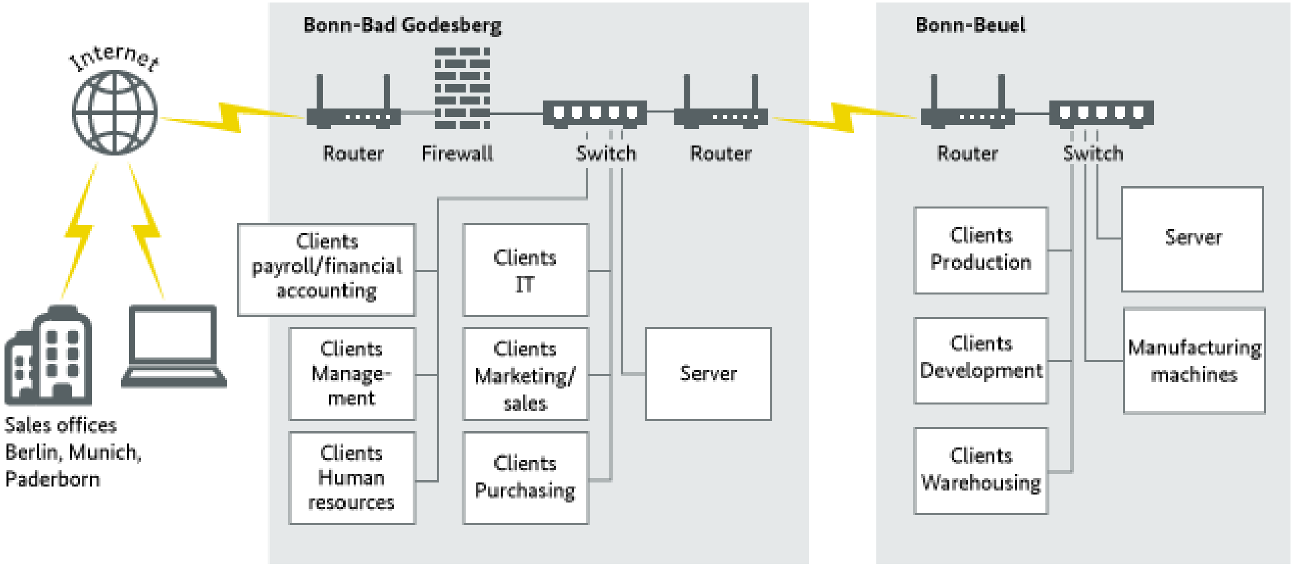


Illlustration 7: RECPLAST GmbH’s organisational chart

In Unit 2.3: *Identifying Business Processes and Information,* you will learn more about the business processes carried out in this organisational structure.

IT systems and networking

RECPLAST's two locations in Bonn are connected by a leased line. Its offices outside of Bonn have a secure connection to the company's network. The following network diagram provides an initial impression of RECPLAST's IT systems and the network connections that link them.



Illlustration 8: Simplified network diagram of RECPLAST GmbH

In units 3.5: Establishing a Network Diagram and 3.6: *Identifying IT Systems, you will learn more about the IT systems depicted, how they are connected, and how they relate to the business processes and applications of RECPLAST GmbH.*

Unit 2.2: Grouping Objects

The goal of structural analysis is to identify the objects for which appropriate safeguards must be established in a corresponding security concept and describe how they interact. It is crucial that all the objects in need of protection be adequately defined.

Before this task is covered, it is important to note the following:

If your organisation already has overviews of the elements to be identified in this context – inventories, business process models, or network diagrams, for example – you should evaluate them during your structural analysis.

The aim of structural analysis is not to obtain an exhaustive inventory of all the technical components in use. Instead, all the objects you identify in specific areas should be **assembled into suitable groups**, which you will then be able to treat as single objects in the subsequent steps of concept development. It makes sense, for example, to group together IT systems that have identical (or similar) configurations and are used for the same tasks.

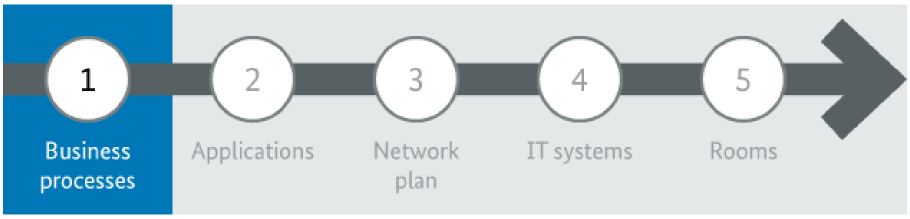
As a rule, you should group components together when **all** of the following applies:

- are of the same type,
- have identical or almost identical configurations
- They are integrated into the network in the same (or almost the same) manner
- They are subject to the same surrounding administrative and infrastructural conditions
- They use the same applications
- They have the same **protection requirements**

It is generally advisable to assemble clients in groups. That said, servers can also be grouped if they meet the criteria listed above. This applies to servers designed for redundancy, for example. [delete] Other typical examples of elements suitable for grouping are offices that have the same equipment and purpose, and the connections between a given switch and the clients of a group. The sections that follow cover additional examples of helpful groupings.

Take care in determining the objects you wish to group. If you group together components that have different protection requirements, this may lead to security vulnerabilities.

Unit 2.3: Identifying Business Processes and Information



A security concept should protect an organisation's **critical information**. What is critical typically becomes clear when examining **business processes**: What information is necessary to enable these processes to run smoothly? What information requires a high level of confidentiality and should thus only be accessible to those authorised? What information is subject to data protection requirements or legal obligations (those meant to ensure the verifiability of business processes, for example)?

In many cases, it is possible to fall back on existing overviews (or “process maps”) of essential business processes or specialised tasks, or to identify processes based on task descriptions or an organisational chart.

Presentation of results

Tables offer a clearly arranged way to list the processes and information you identify. For each business process, you should include the following details:

- A unique identifier (a number or abbreviation)
- A name for the process
- A brief description of its purpose, the workflows involved, and the information processed
- Those responsible for the process
- Key applications that the process requires

Example

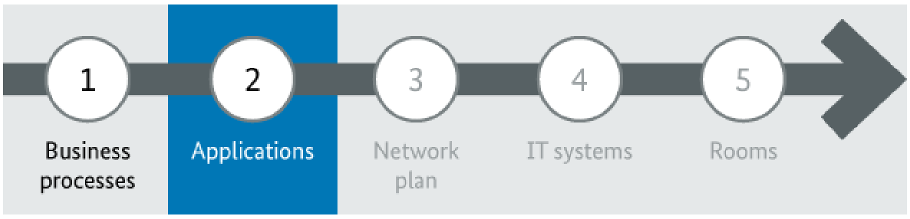
The following table displays some of the business processes identified at RECPLAST GmbH. They are identified as such by the prefix “BP” and are labelled with sequential numbers.

The applications required for a process are assigned in a separate table.

Identifier	Name (type) and description of process, information used	Person responsible	employees
BP001	**Production (core business):** RECPLAST's production of plastic items covers all the corresponding phases, from the provision of materials to the warehousing of finished products. Its production activities also include internal transportation routes, the manufacturing of various components, and related packaging. All the information involved is processed based on orders, stock levels, and bills of materials.	Head of production	All employees
GP002	**Quotation processing (supporting process):** Quotation processing handles the product enquiries received from customers. In most cases, customer enquiries are received via formless e-mails and faxes. Quotations are created electronically, but sent to customers in writing through the post. This area processes quotations, customer data, stock levels, and enquiries.	Head of quotation processing	Sales department
GP003	**Order processing (core business):** Customers typically submit their orders by fax or e-mail. All these documents must be printed out and entered in an electronic format. A customer only receives an order confirmation when one is expressly requested or the production process deviates from the usual production schedule. Order processing makes use of orders, customer data, and stock levels.	Head of order processing	Sales department
GP004	**Purchasing (supporting process):** The purchasing department orders all necessary items that are not required for the production process. This department also negotiates external contracts, formulates IT contracts, and procures consumables used for organisational purposes (paper, toner, etc). The information it uses includes stock levels, notifications of requirements, and information on suppliers.	Head of purchasing	Purchasing
GP005	**Material planning (core business):** The material requirements planning department procures all the materials required in production (plastics, screws, bags, etc). Framework agreements are typically in place for these materials. Planning is conducted in this area based on annual estimated quantities and various order values.	Head of material planning	Material planning, production

Table 1: List of business processes at RECPLAST GmbH (excerpt)

Unit 2.4: Identifying applications



The applications you need to identify are the **IT solutions** that support your business processes and the completion of specialised tasks. They demand a certain **minimum level of protection** due to their requirements with regard to confidentiality, accuracy, authenticity, and availability. Discussions and workshops involving users, those responsible for business processes and applications, and IT department specialists are useful in identifying applications that are essential in this context and thus need to be documented during structural analysis.

For each application identified as essential, you should enter the **following details** into a corresponding table:

- A unique identifier (a number or abbreviation)
- A name for the application
- A brief description of its purpose and the information processed
- Those responsible for the application
- Those who use the application

In addition, you will need to document the dependencies that exist among your applications, business processes, and specialised tasks – that is, identify the processes and tasks in which a given application is used.

When identifying applications, be sure to apply an **appropriate level of granularity**. It is generally not advisable, for example, to break a Microsoft Office product down into its constituent parts (word processing, presentations, spreadsheets) and describe them individually. An overly granular approach will produce an excessive amount of objects to be covered, which will result in unnecessary effort in the subsequent phases of designing your security concept. Not being granular enough, on the other hand, will prevent you from achieving the necessary differentiation, and in particular from defining the safeguards required.

Example: applications at RECPLAST GmbH

A complete overview of all the applications of significance in RECPLAST's business processes would go beyond the scope of this course. The following tables thus contain only an excerpt in order to illustrate how you can document applications and their connections to your business processes.

Name	Name and description of application	Number	Users	Admin / person responsible
A001	**Word processing, presentations, spreadsheets:** All business information – correspondence, analyses, and presentations, for example – is processed in a Microsoft Office product.	290	All employees	IT operations
A002	**Lotus Notes:** This application is used by all employees to manage e-mails, appointments, and contacts.	290	All employees	IT operations
...				
A009	**Order and customer management** This database-supported application is used to process customer master and order data and prepare information for production and deliveries.	55	Sales and marketing	Sales and marketing
A010	**Active Directory:** This application is designed to assist IT operations specialists in their work and reduce redundant user entries. It processes and stores information on all those who use the company's IT systems in terms of their group assignments, rights, and authorisation characteristics. This application is available through both domain controllers.	2	Administra tors	IT operations
...				
A013	**BG printing service:** This service enables all the company's employees in Bad Godesberg to use the printers there. It is available on the print server in Bad Godesberg, but can also be started on the print server in Beuel when necessary.	1	All employees in Bad Godesberg	IT operations
A014	**Beuel printing service:** This service enables all the company's employees in Beuel to use the printers there. It is available on the print server in Beuel, but can also be started on the print server in Bad Godesberg when necessary.	1	All employees in Beuel	IT operations

Name	Name and description of application	Number	Users	Admin / person responsible
A015	**Firewall:** This application oversees communications between the company network and the public Internet; it also facilitates encrypted communications among RECPLAST's sales offices through VPN tunnels.	1	All employees	IT operations
A016	**Telecommunications forwarding:** The two interlinked telecommunications systems in Bad Godesberg and Beuel forward incoming and outgoing calls and faxed documents. They also maintain a telephone directory.	2	All employees	IT operations

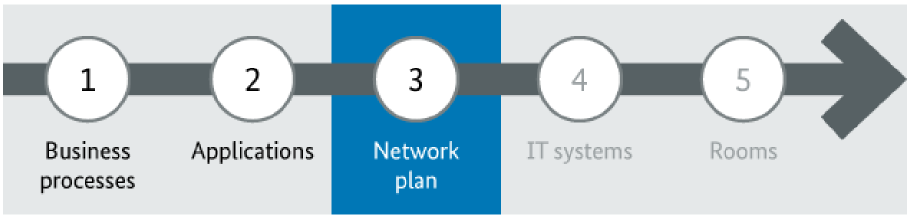
Table 2: List of applications (excerpt)

The following table displays an excerpt of the business processes in which these applications are used:

Business process	Application							
	A001	A002	A003	A004	A005	A006	...	A013	A014
GP001 *Production*		X	X	X		X		X	X
GP002 *Quotation processing*		X	X	X	X			X	X
GP003 *Order processing*	X	X	X	X	X			X	X
GP004 *Purchasing*		X	X	X	X			X	X
GP005 *Material planning*	X	X	X	X	X			X	X

Table 3: Mapping of applications to business processes

Unit 2.5: Establishing a Network Diagram



A network diagram is a graphical overview of the components of a network and their interconnections. On a detailed level, a diagram of this kind should contain the following objects at minimum:

- The **IT systems** on the network, including computers (clients and servers), network printers, and active network components (switches, routers, wireless access points)
- The **connections linking these IT systems** via LAN (e.g. Ethernet), backbone technology (e.g. ATM), and so on
- The **external connections of these IT systems**; here, the type of connection should also be indicated (Internet connection, DSL, etc)

In most cases, your IT admins will have already created a network diagram of this kind. A network and the components in use are, however, subject to frequent changes, which means that existing diagrams may no longer be up-to-date.

This is why you should review the network diagram you plan to use for your structural analysis to determine whether all the information is still accurate. Ask your company's administrator, network and systems manager, or another person responsible for IT about how current the plans at your disposal are.

Many companies and government agencies use software that can automatically generate a network diagram based on the circumstances found on a given network. However, such illustrations typically contain far more information than what is actually required for structural analysis. In particular, they also fail to group together the IT systems at hand in a suitable manner. For these reasons, we recommend “condensing” diagrams of this kind by limiting their information to what is necessary and taking a purpose-oriented approach to grouping their individual components.

Example

The figure below depicts a network diagram that has been condensed as described above at RECPLAST GmbH. The following groups (among others) have been formed:

- The desktop computers in the **production** and **warehousing** departments have been grouped together because they essentially have the same components and are used to access data volumes that are largely identical.
- The three **sales offices** have standard IT equipment, matching tasks and regulations, and identical means of accessing the company network. In a certain sense, they are comparable to home offices from which employees telecommute. They have thus been assembled into a group.
- The **fax machines** and **telecommunications systems** (which constitute non-networked components) used across the company's locations have been added to their own groups because standard organisational rules apply to the use of these devices.
- **Laptops** have been grouped together apart from each department's workstation computers because the possibility of mobile use requires employees to observe additional security standards.

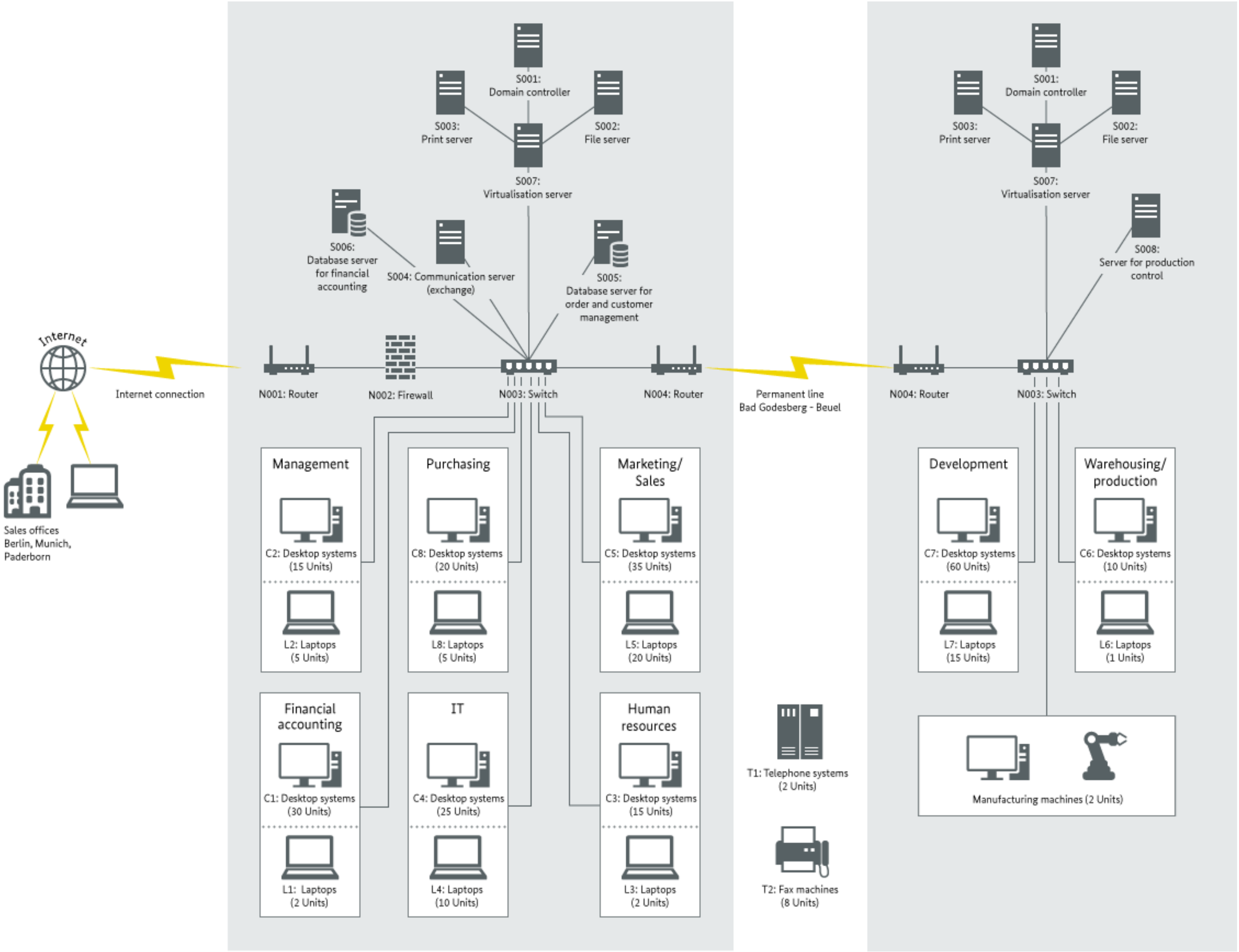
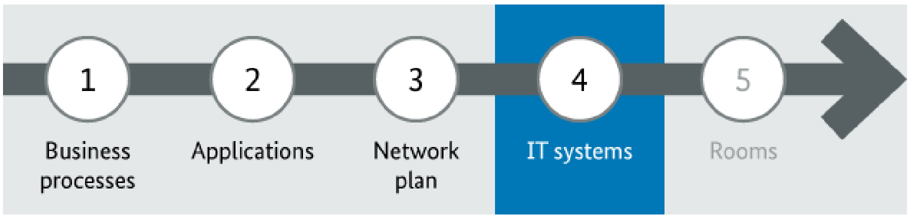

S001: Domain controller
S003: Print server
S002: File server
S007: Virtualisation server
S006: Database server for financial accounting
S004: Communication server (exchange)
S005: Database server for order and customer management
Internet
Internet connection
N001: Router
N002: Firewall
N003: Switch
N004: Router
Permanent line Bad Godesberg - Beuel
Sales offices Berlin, Munich, Paderborn
Management
C2: Desktop systems (15 Units)
L2: Laptops (5 Units)
Purchasing
C8: Desktop systems (20 Units)
L8: Laptops (5 Units)
Marketing/ Sales
C5: Desktop systems (35 Units)
L5: Laptops (20 Units)
Financial accounting
C1: Desktop systems (30 Units)
L1: Laptops (2 Units)
IT
C4: Desktop systems (25 Units)
L4: Laptops (10 Units)
Human resources
C3: Desktop systems (15 Units)
L3: Laptops (2 Units)
T1: Telephone systems (2 Units)
T2: Fax machines (8 Units)
S001: Domain controller
S003: Print server
S002: File server
S007: Virtualisation server
S008: Server for production control
N004: Router
N003: Switch
Development
C7: Desktop systems (60 Units)
L7: Laptops (15 Units)
Warehousing/ production
C6: Desktop systems (10 Units)
L6: Laptops (1 Units)
Manufacturing machines (2 Units)

Illustration 9: A condensed network diagram

Unit 2.6: Identifying IT Systems



In identifying IT systems, you will compile a list of the IT systems both currently in place and planned at your organisation, along with other IT components in the corresponding information network and their characteristics. In doing so, you will also document the applications to which each IT system is relevant. This is another area where tabular overviews are advisable due to the clearly arranged format they provide.

What systems are considered IT systems?

IT systems include:

- All the computers (clients and servers), groups of computers, active network components, and network printers on a given network, as well as;
- Industrial control systems (ICS), which in turn include:
  - Devices used for control or monitoring purposes in production, such as programmable logic controllers (PLCs), machines that are controlled via wireless networks, and self-driving vehicles, as well as;
  - Workstation computers used to control machines, along with the devices connected to these computers (such as scanners or printers)
- Telecommunications devices, mobile phones, and other mobile devices
- Objects pertaining to the Internet of Things (IoT) – that is, networked devices capable of collecting, storing, processing, and transmitting data; these include web cameras, smart home components, and voice-activated virtual assistants (IT-Grundschutz modules are available for these devices, as well)

What details are required for IT systems?

A tabular overview should contain the following information on every IT system:

- A unique identifier
- In the case of a group, the number of IT systems it contains
- A description (here, it is especially important to cite the system's type and purpose – “personnel administration server” or “router to public Internet”, for example)
- Platform (type of hardware, operating system)
- Location (building and room number)
- Status (planned, in testing, operational)
- The system's users and administrator

To document the relationships among IT systems and applications, it is a good idea to use the type of matrix described in unit 3.4: *Identifying applications* as a means of illustrating the dependencies among business processes and applications.

When dealing with networked IT systems, make sure that the information on your list of IT systems matches that of your network diagram.

Example

The following table presents an excerpt of the IT systems at RECPLAST GmbH. The different letters used as the first characters of the identifiers indicate the different types of IT systems at hand (“S” for server, “N” for network component, etc).

Name	Description of object	Location	Number	Status	Users	Admin / person responsible
N001	**Internet connection router:** This router governs communications between the public Internet and the company's internal network.	BG server room	1	Operational	Administrators	IT operations
N002	**Internet access firewall:** This firewall serves as a protective barrier between the public Internet and the company's internal network.	BG server room	1	Operational	Administrators	IT operations

Name	Description of object	Location	Number	Status	Users	Admin / person responsible
N003	**Switches – distribution:** These switches govern the flow of data between the public Internet and the local network.	Server rooms BG and Beuel	2	Operational	Administrators	IT operations
N004	**Router for BG – Beuel (Bonn):** RECPLAST's two locations in Bonn are connected by a leased line. These routers secure the connection.	Server rooms BG and Beuel	2	Operational	Administrators	IT operations
…						
S020	**Virtualisation server (configuration 1):** Up to 20 virtual servers can be configured on this server. An application is used for the administration of these virtualised systems.	Server rooms BG and Beuel	2	Operational	Administrators	IT operations
S008	**Print server (VM):** A server for printing services, which are controlled centrally.	Server rooms BG and Beuel	2	Operational	Administrators	IT operations
…						
C001	**Workstation computers, purchasing** Standard computers with standard software	BG offices		Operational	Purchasing employees	IT operations
C002	**Workstation computers, executive management** Standard computers with standard software; contain confidential correspondence	BG offices		Operational	Management employees	IT operations
L001	**Laptops, purchasing** Laptops with standard software; suitable for mobile use	BG offices and mobile environments		Operational	Purchasing employees	IT operations
L002	**Laptops, executive management** Laptops with standard software; suitable for mobile use; contain confidential correspondence	BG offices and mobile environments		Operational	Management employees	IT operations
…						
S200 S201	**Alarm systems** Proper functionality is crucial to the protection of all building assets.	Buildings in BG and Beuel	2	Operational	Gatekeepers, occupational safety specialists	Building services
I001 I002	**PLC for injection moulding machine** Programmable logic controller and computer for controlling production machine	Production facility in Beuel	2	Operational	Production employees	IT operations

Table 4: List of IT systems (excerpt)

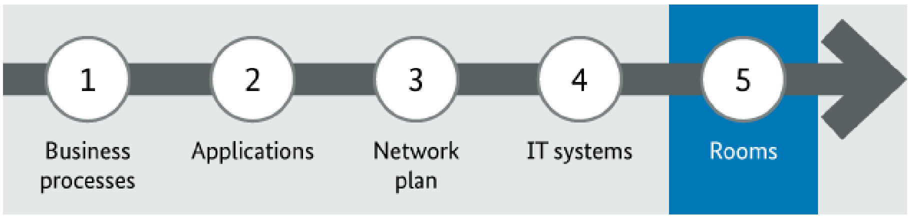
The next table displays some of the network components used by the applications in question:

Name	Description of application	Internet router	Firewall	Switches	Router for BG-Beuel
A001	Text processing, presentation, spreadsheets			X	X
A002	Lotus Notes	X	X	X	X
…					
A009	Order and customer management	X	X	X	X
A010	Active Directory			X	X

Name	Description of application	Internet router	Firewall	Switches	Router for BG-Beuel
...					
A013	BG printing service			X	
A014	Beuel printing service			X	
...					

Table 5: Mapping of applications to network components (excerpt)

Unit 2.7: Identifying Physical Spaces



The extent to which information and related technology is protected always depends on the security of the physical environment in which they are housed, as well. This is why you will need to identify all the buildings and other premises that are of significance in connection with the information and business processes under review during structural analysis. Along with server rooms and other spaces that are explicitly related to IT, these can include the paths traced by communication lines, ordinary offices and training and meeting rooms, and archiving facilities.

To document the relationships among IT systems and physical spaces, it is a good idea to use the type of matrix described inUnit 2.4: as a means of illustrating the dependencies among business processes and applications.

> If your company houses IT systems (data media archives, for example), individual servers, or network coupling devices in secure cabinets, you should also include these cabinets in your inventory of physical spaces.

Example

The excerpt below presents some of the physical spaces identified at RECPLAST GmbH. The list contains two buildings (administration and production), the offices and server rooms located there, and the company's three sales offices. These different spaces have been grouped, assigned sequential numbers, and labelled with the abbreviation “B” (for building) or “R” (room).

Name	Description	Type	Location
GB1	Administrative building	Buildings	Bad Godesberg (Bonn)
GB2	Production building	Buildings	Beuel (Bonn)
...			
R002	Server room, Bad Godesberg	Server room	GB1
...			
R008	Purchasing / sales / marketing offices	Offices	GB1, R. 2.03-2.09
...			
R011	Development department offices	Offices	B2, R. 2.14-2.20

Name	Description	Type	Location
...			
R099	Sales offices	Home workplace	Berlin, Munich, Paderborn

Table 6: List of physical spaces (excerpt)

Alternative approach: starting with IT systems

Identifying physical spaces is the last step of structural analysis. In principle, it is also possible to start by identifying IT systems and establishing a network diagram instead of following the progression recommended here. If you opt for this route, you can make the process of identifying key applications easier by first examining those that are supported by central components (servers, for example) and then those that are assigned to clients and other IT systems.

Unit 2.8: Test questions

If you wish, you can use the following questions to test your knowledge of structural analysis and its importance in the context of the IT-Grundschutz methodology. See the attachment for solutions to the questions. Please note that multiple answers may be correct.

1 **What are objectives of structural analysis within the context of IT-Grundschutz Methodology?**

a Identifying objects that are exposed to particularly significant risks

b Identifying objects that a corresponding security concept needs to cover

c Assembling objects to which the same security measures can be applied into suitable groups

d Determining the objects for which there are appropriate modules in the IT-Grundschutz Compendium

2 **What information can be found in networks that are necessary for a structural analysis?**

a The organisational units involved in drafting the security concept

b The type of connections linking the IT systems in the information network at hand

c The external network connections of the information network at hand

d The type of IT systems in the information network at hand

3 **When would it be useful to group IT systems during a structural analysis?**

a When they have the same protection requirements and similar characteristics (operating system, network connection, supported applications)

b When these systems have their own appropriate modules in the IT-Grundschutz Compendium

c When they share the same premises

d When the total number of objects documented is growing too large

4 **Which of the following tasks are part of structural analysis according to BSI Standard 200-2?**

a Grouping together the components of an information network in a suitable manner

b Modelling the business processes and specialised tasks within an information network c Checking whether the IT in use provides adequate support to the business processes and specialised tasks at hand

d Documenting the information, business processes, applications, IT systems, communication connections, and spatial conditions in the information network at hand

5 **What information on IT systems must be documented during a structural analysis?**

a Type and purpose of use

b Supplier and price

c Users and administrator

d Location (building and room)

6 **What applications must be documented during structural analysis?**

a All the applications installed on the IT systems of the information network at hand

b All applications that are required by at least one of the business processes documented

c All applications for which a valid licence is available

d All applications that are used by at least 20% of an organisation's employees

Lesson 3: Determining protection requirements

How much protection do the information network at hand and its target objects require? How can you render well-founded and comprehensible assessments of protection requirements? Which target objects need a higher level of security, and for which are the ordinary standards sufficient?

In determining protection requirements, the goal is to answer these questions as a means of defining security demands and managing your selection of appropriate measures for the individual target objects in the information network under review.

In this lesson, you will learn how to proceed in determining protection requirements. In particular, it covers the following:

- How to define categories of protection requirements using damage scenarios
- The order in which it makes sense to determine protection requirements for the different types of target objects in the information network at hand
- How dependencies among target objects can impact the results of your determination of protection requirements
- The conclusions that can be drawn from the results of your determination of protection requirements

When implementing the Basic Protection, only the basic requirements are mandatory for the information network under review. As a result, it is not necessary to determine protection requirements when following this variant of the IT-Grundschutz methodology.

Unit 3.1: Basic Definitions

When determining protection requirements, it is important to consider the damage that can result from violations of the **basic values** of confidentiality, integrity, and availability. This is applicable when:

- Confidential information is accessed or passed on in an unauthorised manner (violation of **confidentiality**)

- Information is no longer correct or systems no longer function properly (violation of **integrity**)
- Authorised users are prevented from accessing systems and information (violation of **availability**)

The protection a given object requires with regard to each of these basic values is thus based on the extent of the damage corresponding violations can cause. Since the extent of potential damage can typically not be determined in advance, you should define a number of categories suitable for your purposes and use them to differentiate between various levels of protection. The IT-Grundschutz methodology recommends three **categories of protection requirements**:

- **Normal:** The effects of the damage are limited and manageable.
- **High**: The effects of the damage may be considerable.
- **Very high**: The effects of the damage may be catastrophic enough to threaten an organisation's existence.

The possible ramifications of a violation of the basic values can pertain to various **damage scenarios**:

- violations of laws, regulations or contracts,
- Impairment of the right to informational self-determination
- Impairment of a person's physical integrity
- Impairment of one's ability to perform tasks
- Negative internal or external consequences
- financial consequences.

The importance of each scenario differs from organisation to organisation. Companies, for example, are particularly concerned about the financial consequences of such damage; at a certain level, their very existence may be at risk. For a government agency, on the other hand, it may be especially important to avoid negative external consequences that could impact its reputation in the eyes of the public.

Unit 3.2: Protection need categories

When do objects have normal, high, and very high protection requirements?

It is not possible to provide a universal answer to this question for every damage scenario. For an initial differentiation of the categories at hand, please refer to chapter 8.2.1 of BSI Standard 200-2: *IT-Grundschutz Methodology*. You can use the relatively general definitions provided there as a starting point before adapting and supplementing them to reflect the particular circumstances at your organisation.

For example, the chapter specified includes the following statement regarding the “normal” category of protection requirements and the damage scenario “financial consequences”:

- “The financial loss is tolerable for the organisation.”

But what does “tolerable” mean to a particular company? For a very large company, several million euros may not have a major impact; for a small or midsize company, however, damage on this scale can lead to bankruptcy. When differentiating among damage categories, you will thus need to factor in the particular characteristics of the organisation in question, including in regard to:

- A company's profits or revenues (or a government agency's allotted budget) in connection with the “financial consequences” scenario
- The availability of a backup procedure should one fail in connection with the “impairment of the ability to perform tasks” scenario

Example

For the example company RECPLAST GmbH, the following provisions have been established regarding the “financial consequences” and “impairment of the ability to perform tasks” scenarios:

- Normal protection requirements:
  - “The potential financial damage is less than €50,000.”
  - “The processes at RECPLAST will under no circumstances be significantly impaired. Outages lasting for more than 24 hours can be tolerated.”
- High protection requirements:
  - “The potential financial damage is between €50,000 and €500,000.”
  - “The processes at RECPLAST will be significantly impaired. Outages must not last longer than 24 hours.”
- Very high protection requirements:
  - “The potential financial damage is greater than €500,000.”
  - “The processes at RECPLAST will be so severely impaired that outages lasting longer than two hours cannot be tolerated.”

Unit 3.3: Approach and Inheritance

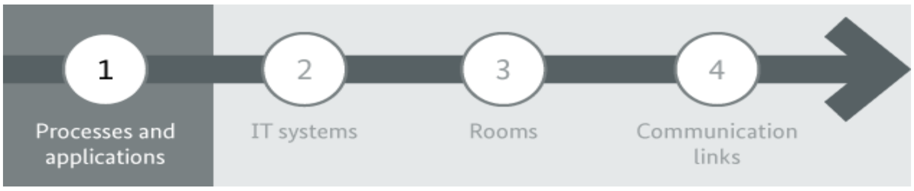
The objects in a given information network are used to support business processes and applications. As a result, the protection requirements of a particular object depend on those of the business processes and information that require said object in order to function.

This is why the protection requirements of these business processes and related information need to be determined first. Their protection requirements are then inherited by the corresponding applications, IT systems, physical spaces, and communication connections.

Taking IT systems as an example, this **inheritance** can be differentiated based on the **following cases**:

- In many instances, the highest level of protection required among all the applications that require a given IT system can be adopted (also known as the **maximum principle**).
- When an application requires the results produced by another application, the protection requirements of the former are passed on to the latter. If these two applications run on different IT systems, the protection requirements of the receiving system must be passed on to the system supplying the results **(dependency perspective)**.
- The protection requirements of an IT system can be higher than those of its individual applications (**cumulative effect**). This applies, for example, when multiple applications with normal protection requirements run on a given server. While the failure of one of these applications would be manageable, all of them failing at once could result in significant damage.
- The protection requirements of an IT system can be lower than those of its corresponding applications if an application with high protection requirements is distributed across multiple systems and the IT system in question only runs a small number of its components (**distribution effect**). In the case of applications that process personal data, those components that only use data in pseudonymised form (for example) are less critical.

Unit 3.4: Determining Protection Requirements for Processes and Applications



In order to estimate the damage that can result from violations of integrity, confidentiality, or availability in processes and applications, you should develop damage scenarios that are realistic **from a user's perspective**.

Here, formulating **"what if" questions** for each damage scenario can be helpful. For example, what if confidential business data from a financial accounting application is made public?

- What laws or regulations would this violate? What legal penalties or other consequences could result from this incident?
- Would any individuals be impaired in their right to informational self-determination? If so, what would the ramifications be?
- To what extent would the company's processes be impaired?
- Could the company's reputation be damaged, and what would the ramifications be?
- Could the incident have financial consequences, and if so, on what scale?

The appendix of BSI Standard 200-2 contains example questions for each damage scenario that you can adapt and supplement in line with the protection requirements determined at your organisation.

The next step involves answering the questions you have developed for your damage scenarios for all the applications you identified during structural analysis. This will enable you to assess the protection requirements of these applications in terms of the three basic values (confidentiality, integrity, and availability).

When estimating damage, you should be sure to involve the users of each application and those responsible for it. These individuals typically have in-depth knowledge of the damage that can occur when an application fails or inaccurate data are used. That said, those within the corresponding project group and the employees you consult may have differing opinions on the level of protection required. If you cannot come to a consensus, such decisions must be made at the executive level.

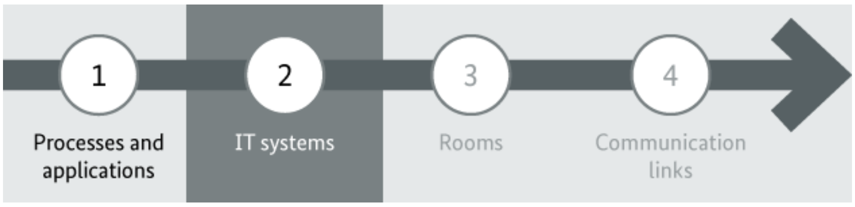
It is important that you provide justification for the protection requirements you determine, and that you be thorough enough to enable others – at the executive level, for example – to follow the decisions you take at a later point in time (and make corrections if necessary). In many cases, executives, users, and department heads can have varying views of how important a given application is to certain business processes.

The example below presents the protection requirements determined for a number of applications at RECPLAST GmbH.

Name	Description of application	Objective and protection requirements	Rationale
A001	Text processing, presentation, spreadsheets	Confidentiality: **Normal**	The Office application itself contains no information
		Integrity: **Normal**	The Office application itself contains no information
		Availability: **Normal**	The application is installed locally, and reinstalling it does not take long. The licences are stored in a secure manner. Downtime of 24 hours or more is acceptable.
A002	Lotus Notes	Confidentiality: **High**	This application manages e-mails with confidential content. Information on business contacts and meetings with partners or customers is confidential.
		Integrity: **Normal**	In most cases, it is easy to identify inaccurate data.
		Availability: **Very high**	E-mails, contact data, and appointments are essential to the organisation's business processes. Outages lasting for more than two hours cannot be tolerated.

Table 7: Protection requirements of applications (excerpt)

Unit 3.5: Determining the Protection Requirements of IT Systems



IT systems are used to support applications. As a result, the protection requirements of an IT system depend to a large extent on those of the applications that require the system in order to run. The protection requirements of an application are inherited by the corresponding IT system as described above.

Here are some notes on special types of IT systems:

- In most **virtualised infrastructures**, multiple IT systems run on a virtualisation server. The protection requirements of these individual virtual systems are derived from those of the applications at hand; the protection requirements of the virtualisation server itself are initially based on the maximum principle. However, if multiple instances of damage could lead to a greater amount of overall damage, the protection requirements of the virtualisation server can rise due to the cumulative effect. When it comes to ensuring availability, if the virtualisation concepts at hand lead to redundancies, the protection requirements of the virtualisation server can be set back to a lower level due to the distribution effect.
- You should discuss the protection requirements of **ICS components** with those responsible for such systems based on the purpose of their use. Here, it can be helpful to adjust your defined categories of protection requirements to the particular conditions of a production environment.
- For **other devices** (e.g. those pertaining to the Internet of Things), you must first identify the business processes and applications for which they are used. To determine the protection requirements of a given device, examine the damage it could cause to the respective business process. You should only document devices that have a substantial impact on information security and assemble them into groups whenever possible.

The protection requirements of IT systems should also be defined in terms of the three basic values (confidentiality, integrity, and availability) and then documented – in a tabular format, for instance. Here is an example:

Bezeich-nung	Beschreibung des Systems	Schutzziel und Schutzbedarf	Begründung
S007	Virtualisation servers	Confidentiality: **High**	*Maximum principle*: The domain controller contains Active Directory, and with it the login information of all the company's employees.
		Integrity: **High**	*Maximum principle*: The file server manages files whose accuracy must be ensured for the company's business operations.
		Availability: **High**	*Cumulative effect*: Both the domain controller and the file server have high availability requirements. This results in very high protection requirements for the virtualisation server. However, all the virtualised systems can be made available on the other virtualisation server in short order. Due to the *distribution effect*, the protection requirements at hand are merely “high”.
N001	Internet router	Confidentiality: **High**	Confidential information is transmitted through this Internet connection even when a customer or business partner does not support encrypted communications.
		Integrity: **Normal**	In most cases, it is easy to identify inaccurate data.
		Availability: **Normal**	A failure of this Internet connection can be tolerated for 24 hours.
N002	Firewall	Confidentiality: **High**	Confidential information is transmitted through this Internet connection even when a customer or business partner does not support encrypted communications. The firewall also establishes encrypted connections to the company's sales offices.
		Integrity: **Normal**	In most cases, it is easy to identify inaccurate data.
		Availability: **Normal**	A failure of this Internet connection can be tolerated for 24 hours.
S200	Alarm systems	Confidentiality: **Normal**	The alarm systems do not process any confidential information.
		Integrity: **Very high**	To ensure building security, it is essential that the alarm systems function properly.
		Availability: **Very high**	To ensure building security, it is essential that the alarm systems function properly.

Table 8: Protection requirements of IT systems (excerpt)

Unit 3.6: Defining Protection Requirements for Physical Spaces

1
Processes and applications
2
IT systems
3
Rooms
4
Communication links

In determining the protection requirements of physical spaces, you will need to factor in all the spaces and properties you identified during structural analysis that are relevant to the information, applications, and IT systems in the information network under review.

Principles of inheritance must be taken into account in this area, as well. The protection requirements of a physical space are determined according to those of the IT systems it contains, as well as the requirements of the information and data media that are processed and stored therein. This means you can apply the maximum principle in most cases (as in determining the protection requirements of IT systems). In some situations, however, the large number of objects in a given physical space can lead to protection requirements that are higher for a particular basic value than those of the individual objects (cumulative effect). This can apply, for example, to spaces that house mirrored servers with normal availability requirements: While there are two servers in case one fails, an incident affecting the entire space (a fire, for instance) would impact both servers at once. This does not apply if the two servers are located in different spaces (or even different buildings).

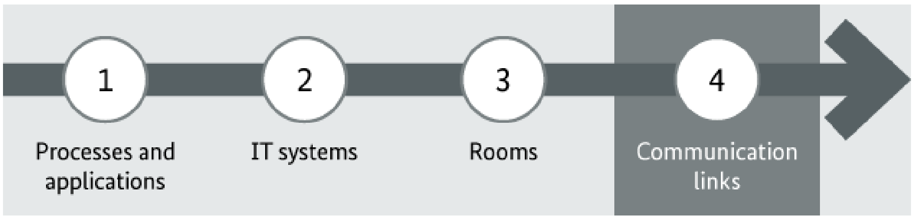
Example

The following table offers an example based on the documentation produced for the protection requirements of the physical spaces at RECPLAST GmbH.

Room			IT systems	Protection requirements		
Title	Type	Location		Confidentiality	Integrity	Availability
BG, R. 1.01	Technology room	GB1	Telecommunications system T1	normal	normal	High
BG, R. 1.02	Server room	GB1	N001 to N004 S001 to S020	High	High	High
Beuel, R. 2.01	Server room	GB2	N004 S008, S020 S040	High	High	High
Beuel, R. 2.10-2.15	Office	GB2	A007, L007	High	normal	normal

Table 9: Protection requirements of physical spaces (excerpt)

Unit 3.7: Defining Protection Requirements for Communication Links



In the next step, you will need to determine the protection requirements of your organisation's communication links. Some connections are exposed to more risk than others and thus need to be secured against internal and external attacks, whether through redundancy or special safeguards.

Critical connections

The following **connections** should be classified as **critical**:

- Connections that lead from a company or government agency to a **public network** (e.g. the Internet or the telephone network) or **through a public space**. Such connections can be used to introduce malware into an organisation's data network, carry out attacks on its servers, or pass confidential data between employees and unauthorised individuals.
- Connections that are used to transmit **information in need of special protection**. Here, the potential dangers include attempts at interception, deliberate manipulation, and fraudulent misuse. Applications that are subject to high availability requirements are particularly affected by the failure of such connections.
- Connections through which confidential information **must not be transmitted**. Personal data, for instance, may only be accessed and processed by an organisation's executives and employees in human resources. This is why efforts must be made to prevent these data from being accessed by unauthorised employees during transmission.

In your documentation, you should point out the critical nature of these connections by highlighting them on your network diagram or compiling a tabular list.

Examples of critical connections

Taking RECPLAST GmbH as an example, the following table shows how critical connections can be documented.

Identifier	Description	Confidentiality	Integrity	Availability
K001	Company network – Internet	**High:** Confidential information could fall into the hands of competitors (for example)	**High:** False information could damage the company's reputation.	**High:** Without this external connection, communication is impossible.
K002	Leased line Bad Godesberg – Beuel	**High:** Confidentiality must be ensured when transmitting internal information.	**Normal:** Information can only be falsified with a great deal of effort.	**High:** The connection is essential in transferring orders to the production department.

Identifier	Description	Confidentiality	Integrity	Availability
K011	Connection for executive workstations	**High:** Management handles confidential correspondence.	**Normal:** Information can only be falsified with a great deal of effort.	**High:** The connection is essential in communicating with business partners.
K012	Connection for HR workstations	**High:** The HR department works with personal data.	**Normal:** Information can only be falsified with a great deal of effort.	**Normal:** The department's work is typically not urgent. Downtime of 24 hours or more is acceptable.
K013	Connection of developer workstations	**High:** The work produced in this area must be kept confidential.	**Normal:** Information can only be falsified with a great deal of effort.	**Normal:** The department's work is typically not urgent. Downtime of 24 hours or more is acceptable.

Table 10: Critical communication links (excerpt)

Unit 3.8: Test questions

If you wish, you can use the following questions to test your knowledge of how protection requirements are determined in accordance with IT-Grundschutz. See the attachment for solutions to the questions. Please note that multiple answers may be correct.

1 **What traditional objectives are recommended when determining protection requirements in accordance with IT-Grundschutz?**

a Authenticity

b Availability

c Confidentiality

d Integrity

2 **In what cases can you forgo determining an IT system's protection requirements in accordance with IT-Grundschutz?**

a When the IT system is to be decommissioned within 18 months

b When the IT system is not used

c When the applications it supports only have normal protection requirements

d When the protection requirements in question were already determined in an audit conducted one year before

3 **What criteria do you need to take into account when determining an IT system's availability requirements?**

a The maximum system downtime that can be tolerated

b The effort required to restore the IT system following a breakdown

c The number of people who use the IT system

d The costs of procuring the IT system

4 **What do you need to consider when determining the protection requirements of an application?**

a The information used in connection with the application

b The application's significance with regard to business processes or specialised tasks

c The relevant risks to which the application is exposed

d The physical environment of the IT system that makes the application available

5 **Under what circumstances can the protection requirements regarding an IT system's availability be lower than those of the applications for which it is used?**

a When the accounting value of the IT system falls below a previously defined threshold

b When the IT system only serves components of the respective applications that have lower protection requirements

c When at least one other redundant IT system is in use that can make the applications available

d When the applications are to be restructured in a manner that will no longer require the IT system within the next three months

6 **When cumulative effects are to be taken into account in determining an IT system's protection requirements, this means that...**

a ...the IT system has higher protection requirements because individual instances of damage could add up to a greater amount of overall damage

b ...the IT system has lower protection requirements because appropriate and mutually complementary safeguards are in place

c ...the protection requirements determined for the IT system also affect the requirements of other IT systems that are connected to the system in question

d ...the IT system's protection requirements cannot be determined until the requirements of the IT systems connected to it are determined

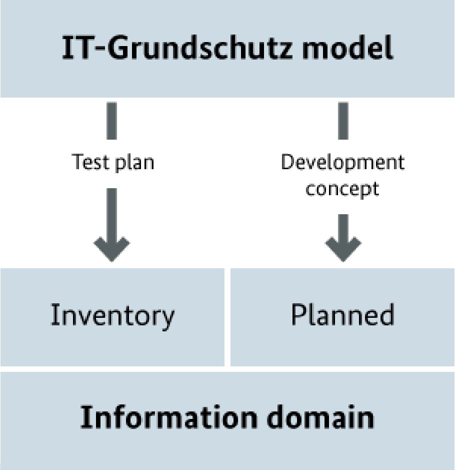
Lesson 4: Modelling in Accordance with IT-Grundschutz

Okay, we have to do something, but what?
Here we will find suitable modules!
Game
Confidential
Patent (Draft)
SOFT-DRINK
SOFT-DRINK
CONFIDENTIAL

In the previous steps, you have identified the individual components that represent target objects for the security concept of the information network under review and assessed their protection requirements in detail. In the next step – **modelling in accordance with IT-Grundschutz** – you will build on these findings in determining the security requirements relevant to the individual target objects at hand. When this is complete, you will have an **IT-Grundschutz model** for your information network.

This model can be used both to evaluate the security of existing systems and procedures and support efforts to take information security into account as necessary when introducing new elements. In short, it provides the following information security support:

- Specifications for a **test plan** for existing elements of the information network at hand
- Specifications for a **development concept** for planned elements



As you develop your IT-Grundschutz model, you will have the support of the **IT-Grundschutz Compendium**. In this lesson, you will thus get to know the structure and content of this document and learn:

- How to use it to create an IT-Grundschutz model for an information network
- How to take special scenarios (involving virtualised systems, for example) into account in a model of this kind
- How to produce suitable documentation on the results of your modelling

Unit 4.1: IT-Grundschutz Modules

The IT-Grundschutz Compendium has a modular structure. This is reflected by the **IT-Grundschutz modules** that form its core, which are each around 10 pages long and describe the typical risks and security requirements of a particular aspect of information security. A module can cover broader topics such as information security and business continuity management, or relatively specialised technical systems that are typically used by companies and government agencies – clients and servers, mobile systems, or industrial control systems, for example.

The modules start with introductory chapters that include notes on the application of the IT-Grundschutz Compendium and an overview of elementary threats. You will learn more about these overviews and their significance in the context of the IT-Grundschutz methodology in 64 Risk analysis.

All the modules are structured in the same way:

- They begin with a **brief description** and delineation of the subject matter at hand.
- The modules then present the specific **threats at hand** using various examples.
- At the heart of each module are the respective **security requirements**, which are separated into three groups:
  - **Basic requirements** that should be fulfilled first
  - **Standard requirements** that can also be met in order to fully implement IT-Grundschutz and a level of security that reflects the current state of the art
  - Specifications for **higher protection requirements**
- Each module concludes with references to further information and a table of cross-references in which the requirements in question are linked to the respective elementary threats.

The requirements describe what MUST or SHOULD be done. Capitalised verbs like these indicate **how compulsory each requirement is**. The following table offers an overview:

Expression	Meaning
MUST	Requirements described in this manner are absolutely essential.
MUST NOT	The action described must never be carried out.
SHOULD	This expression indicates that the requirement in question should normally be met, but can be disregarded for pertinent reasons.
SHOULD NOT	This expression indicates that the action in question should not be carried out in typical cases, but may when pertinent reasons apply.

Table 11: Semantics of the IT-Grundschutz modules

Unit 4.2: Layered model

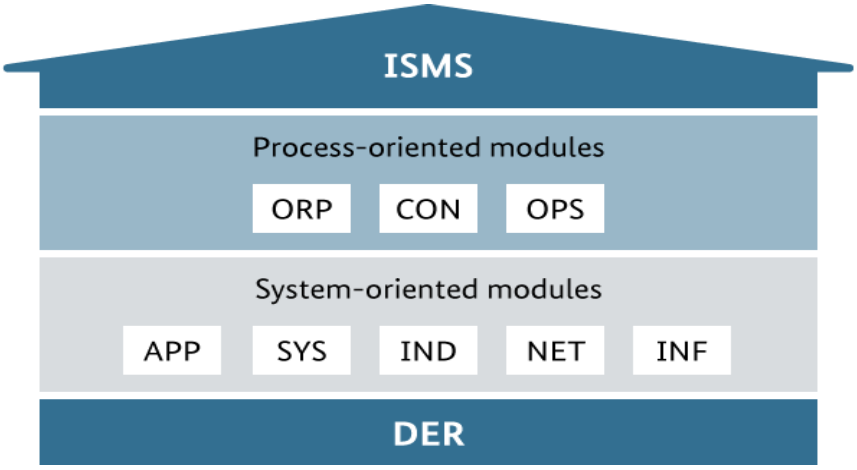


Illustration 10: Layered model

The various IT-Grundschutz modules are structured according to a **layered model** as described below (example modules are cited in parentheses):

Process modules:

- **ISMS**: security management (ISMS.1 *Security management*)
- **ORP:** organisation and personnel (ORP.1 *Organisation*, ORP.2 *Personnel*, ORP.3 *Information Security Awareness and Training*, ORP.4 *Identity and acces management*, ORP.5 *Compliance management*)
- **CON**: concept design and approaches (CON.1 *Crypto-concepts*, CON.2 *Data Protection*, CON.3 *Data backup policy*, CON.6 *Deletion and destroying*, CON.7 *Information security on trips abroad*)
- **OPS**: operations, which is divided into the four sub-layers *in-house IT operations*, *operations run by third parties*, *operations run for third-parties,* and *operational aspects* (OPS.1.1.2 *Proper IT administration*, OPS.1.1.3 *Patch and change management*, OPS.1.1.4 *Protection against malware*, OPS.1.1.5 *Logging*, OPS.2.1 *Outsourcing for customers*, OPS.2.4 *Remote maintenance*)
- **DER:** Detection and reaction (DER.1 *Detection of security-relevant events*, DER.2.1 *Handling security incidents*, DER2.2 *Provisions for IT forensics*, DER.3.1 *Audits and revisions*, DER.4 *Business continuity management*)

System modules:

- **APP**: applications (APP.1.1 *Office products*, APP.1.2 *Web browsers*, APP.3.2 *Web server*, APP.5.1 *General groupware*, APP.5.2 *Microsoft Exchange and Outlook,* APP.6 *General Software,* APP.7 *Development of Individual Software*)
- **SYS**: IT systems (SYS.1.1 *General servers*, SYS.1.2.2 *Windows Server 2012*, SYS.1.5 *Virtualisation*, SYS.2.1 *General client*, SYS.2.3 *Clients under Unix*, SYS.3.1 *Laptops*, SYS 3.2.1 *General smartphones and tablets*, SYS.3.4 *Mobile data media*, SYS.4.4 *General IoT devices*)
- **IND**: industrial IT (IND.1 *Process Control and Automation Technology,* IND.2.1 *General ICS components*, IND.2.3 *Sensors and actuators*)
- **NET**: networks and communications (NET.1.1 *Network architecture and design*, NET.1.2 *Network management*, NET.2.1 *WLAN operations*, NET.2.2 *WLAN* usage, NET.3.1 *Routers and switches*, NET.3.2 *Firewalls*)
- **INF**: infrastructure (INF.1 *General building*, *INF.2 Data centre and server Room*, INF.7 *Office Workplace*, INF.8 *Home workplace*, INF.12 *Cabling)*

Advantages of the layered model

The way in which the modules of the IT-Grundschutz Compendium are arranged offers a number of advantages. Dividing up the various individual aspects of information security reduces the complexity of this subject, for example, and also prevents redundancy. In addition, it makes it easier to update specific aspects of a developed security concept without affecting other parts of the concept.

Meanwhile, the individual layers have been defined in a manner that groups together the respective responsibilities. The ISMS and ORP layers, for example, mainly address an organisation's security management, while INF deals with building services; SYS, NET, and APP, on the other hand, address the administrators, operators, and other individuals responsible for IT systems, networks, and applications (respectively).

The **IT-Grundschutz Compendium** is **updated and expanded on an ongoing basis**. In doing so, the BSI factors in its annual surveys and the desires of relevant users. If you wish to stay up-to-date on IT-Grundschutz or take part in surveys related to its ongoing development, you can subscribe to the BSI's **IT-Grundschutz newsletter**, as well (register here). To engage in a professional dialogue and get the latest information on IT-Grundschutz, you can also check out our group on XING and follow us on Twitter.

Unit 4.3: Approach

During the modelling process, you will need to select the IT-Grundschutz modules required for security in the information network under review. To do so, take a look at the modules of the individual layers before deciding whether and to which target objects each module could be applied. Related support is available in chapter 2.2 *Assignment based on the layered model* of the IT-Grundschutz Compendium.

Ideally, you will have **mapped suitable IT-Grundschutz modules to all the target objects** in your information network when this process is complete. For any target objects for which **no module presents an adequate match**, you will need to perform a risk analysis. The threats and security requirements identified during risk analysis can then be assembled into a user-defined module.

During modelling, you should also take the following considerations into account:

- The **process-oriented modules** describe aspects that encompass the technical aspects of a given information network and typically need to be regulated in a uniform manner. As a rule, these modules should thus be applied once for each information network. The modules on information security management, the organisation of IT operations, training personnel and raising awareness, and detecting and responding to security incidents are especially important.
- The **system-oriented modules** relate to certain technical objects and are to be applied to every technical system (or group of technical systems) addressed in each module. This can include specific applications, IT systems (e.g. clients, servers, or mobile devices), objects pertaining to industrial IT, networks, and infrastructure objects (data centres and other physical spaces, cabling, etc).
- For a number of technical systems, **multiple modules should be applied** to cover all the security requirements relevant to each system. For clients and servers, for example, there are operating-system-agnostic modules (SYS.2.1 *General client*, SYS.1.1 *General server*) that describe the basic security requirements of these systems. There are also operating-system-specific modules (such as SYS.2.2.3 *Clients under Windows 10* and SYS.1.2.2 *Windows server 2012*) that complement the general modules by presenting the particular requirements relevant for the operating system in question. For a web server running on a variant of UNIX, the following three modules should be included in the respective IT-Grundschutz model:
  - SYS.1.1 *General server*
  - SYS.1.3 Server under Unix

  - APP.3.2 *Web server*

- **Virtual systems** are to be modelled in the same way as physical systems, meaning that their functions, operating systems, and the applications and services they provide must be taken into account. If a UNIX server is run as a virtualisation server, for instance, the three modules SYS.1.1 *General server*, SYS.1.3 Server under Unix and SYS.1.5 *Virtualisation* must be applied. The typical modules for servers must also be applied to each of the virtual servers provided by this physical server. There is no IT-Grundschutz module that is appropriate for virtualisation servers that are based on special hardware (also referred to as “bare metal servers”). IT systems of this kind should thus be marked for risk analysis.

Not every module is relevant in every situation. You will obviously only need to apply the module CON.7 *Information security on trips abroad* if such trips are commonly taken at your organisation. You can also forgo special technical modules like SYS.2.2.2 *Clients under Windows 8.1* if your organisation does not use this type of IT system. You should nevertheless cite sufficient reasons why you have not applied certain modules; they need not be lengthy, but should be meaningful.

Unit 4.4: Documentation

For an example of how you can document your modelling, consider the following excerpt from the modelling performed at RECPLAST GmbH. In the *Relevance* column, you can indicate whether modules are of importance to the information network at hand, and then explain your decision under *Rationale*. If you classify a module as irrelevant, an adequate explanation is essential.

Module	Target objects	Relevance	Rationale	Contact persons
APP.5.2 *Microsoft Exchange and Outlook*	S004	Yes		IT operations
INF.1 General building	GB1, GB2	Yes		Building services
INF.2 *Data centre and server room*	R002	Yes		IT operations
INF.7 *Office work*place	R008 bis R011	Yes		
INF.8 *Home Workplace*	R099	Yes	The company's sales offices are treated as home offices.	
INF.12 *Cabling*	Informationsverbund	Yes		
IND.2.2 *Programmable logic controller (PLC)*	I001	Yes		
SYS.1.5 *Virtualisation*	S007	Yes		IT operations
SYS.3.1 *Laptops*	L001 bis L008	Yes		IT operations
OPS.3.1 *Outsourcing for service providers*		No	The company does not offer services of this kind.	

Table 12: Documentation of IT-Grundschutz modelling

While citing contact persons is optional during modelling, it can lay the groundwork for later phases of the methodology (especially the IT-Grundschutz check). When selecting the relevant individuals, it can also be helpful to include information on their roles and responsibilities within the modules at hand.

Unit 4.5: Adapting Requirements

As mentioned previously, the IT-Grundschutz modules describe requirements that an organisation MUST or SHOULD implement. This means they illustrate **what** needs to happen, but not **how**. When creating concepts for both security and testing, it is necessary to formulate security measures that are suitable for meeting each individual requirement. To aid this process, most of the modules of the IT-Grundschutz Compendium contain **implementation recommendations**.

The measures through which a given requirement is to be met must be **appropriate**. In more specific terms, this means:

- They must provide **effective** protection against potential threats and cover the protection requirements identified
- They must be **applicable** – that is, implementing them must be feasible without disproportionately impairing organisational processes or rendering other security measures ineffective
- They must be **practicable** – that is, easy to understand and apply and not prone to errors
- They must be **acceptable**, which includes being accessible, non-discriminatory, and incapable of placing anyone at a disadvantage
- It must be possible to implement and maintain them in a **cost-efficient** manner; the resources their implementation requires must thus be proportionate to the value of the objects to be protected

When implementing the Standard Protection, all the standard requirements of each relevant module typically need to be met along with the mandatory basic requirements. There may be exceptions in isolated cases, however; a requirement may not be relevant, for instance, or fulfilling it may present a conflict in meeting other requirements. This may occur in connection with basic requirements, as well. You will need to cite an understandable rationale for any such deviations. In cases where requirements are relevant but cannot be met with a reasonable amount of resources, you should define suitable alternative solutions.

Unit 4.6: Test questions

If you wish, you can use the following questions to test your knowledge of modelling in accordance with IT-Grundschutz. See the attachment for solutions to the questions. Please note that multiple answers may be correct.

1 **What tasks do you need to perform during modelling in accordance with IT-Grundschutz?**

a You must use the IT-Grundschutz modules to map the information network identified during structural analysis.

b You must draw up a security architecture for the information network under review.

c You must mark target objects that cannot be adequately modelled for subsequent risk analysis.

d You must check whether IT-Grundschutz modules are relevant to the information network under review.

2 **What information does an IT-Grundschutz module contain?**

a Details on specific threats

b Descriptions of standard security measures

c References to further information

d Security requirements pertaining to a given situation

3 **What tasks do you need to perform after determining which modules will be applied to your information network and its individual target objects during modelling?**

a You must define measures through which the requirements at hand can be met.

b You must check whether alternatives are necessary for individual requirements that cannot be met with a reasonable amount of resources in the application context at hand.

c You must adjust the protection requirements determined for target objects for which the fulfilment of said requirements seems unrealistic.

d You must document the results of the modelling process.

4 **What should you bear in mind when selecting and adjusting security measures based on the respective requirements?**

a How cost-efficient the measures are

b How effective the measures are

c How innovative the measures are

d How user-friendly the measures are

5 **Which statements regarding the application of modules to servers apply?**

a The module SYS.1.1 *General Server* should only be applied when there is no operating-system-specific module for the server in question.

b Along with module SYS.1.1 *General Server*, the relevant operating-system-specific module should always be applied.

c When special modules are available for server applications (web or database servers, for example), the relevant operating-system-specific module does not need to be applied.

d For virtualisation servers, the module SYS.1.1 *General Server* and the relevant operating-system-specific module must both be applied along with the module for virtualisation servers.

6 **To what target objects does the module ISMS.1 *Security management* need to be applied during modelling?**

a It MUST be applied separately to each location of a significant size within the information network at hand.

b It MUST be applied once to the entire information network.

c It is only relevant if the information network is of a certain minimum size.

d It MUST be applied separately to every sub-network identified during structural analysis.

Lesson 5: IT-Grundschutz Check

Are the information and IT at my organisation sufficiently protected? What still needs to be done?

The IT-Grundschutz check is an effective means of answering these questions. In principle, the approach it follows is quite simple: You compare the security measures you have already implemented against the requirements of your IT-Grundschutz model (which you determined previously with the help of the IT-Grundschutz Compendium) to assess the level of security you have achieved thus far and identify potential improvements.

Proceeding systematically, you can fall back on the **results of the steps you have already completed**:

- During structural analysis, you documented the information, IT systems, physical spaces, and communication connections at your organisation, along with the applications these elements support.
- You then determined the protection requirements of your applications, IT systems, physical spaces, and communication connections.
- Through subsequent modelling, you assembled a **test plan** (your IT-Grundschutz model) for your information network and its target objects by selecting and specifying the modules to be applied.

This test plan is what you will use for your IT-Grundschutz check, which involves assessing the extent to which the requirements relevant to each IT-Grundschutz module are currently met by appropriate technical and organisational measures for each target object.

In this lesson, you will learn:

- How to prepare an IT-Grundschutz check
- What to keep in mind when carrying it out
- How to document the results

Unit 5.1: Requirements

An IT-Grundschutz check is a **target-actual comparison** of the requirements placed on a given information network (or one of its components) and the measures currently implemented.

The foundation of an IT-Grundschutz check is the **IT-Grundschutz model** you assembled for your information network during modelling based on the target objects at hand and your protection requirements. In this model, you have determined which modules (and corresponding sets of requirements) are to be applied to the individual target objects of your information network.

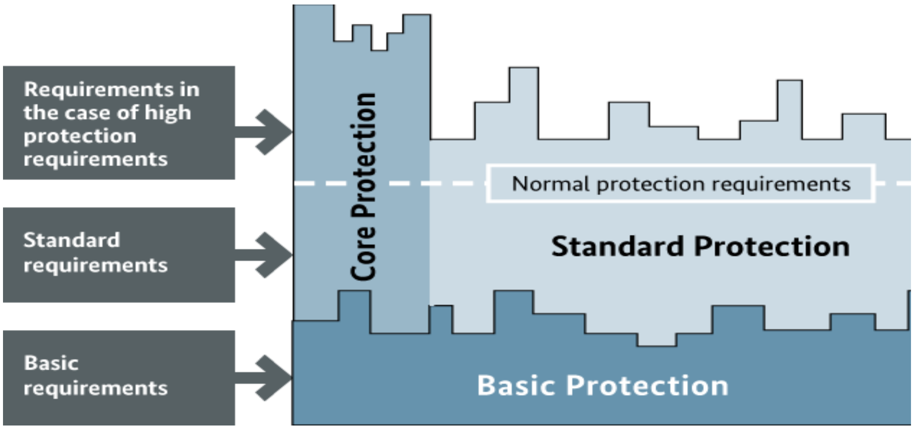


Illustration 11: Requirements of the IT-Grundschutz modules and corresponding approach variants

The modules contain three types of requirements: basic, standard, and those necessary for an increased level of protection. The requirements you incorporate into your IT-Grundschutz check will depend on your approach to implementing the IT-Grundschutz methodology:

- If you plan to implement the Basic Protection, you will only need to fulfil the basic requirements.
- If you are implementing the Standard and Core Protection, you will also need to factor in the standard requirements.
- The requirements covered herein regarding higher levels of protection are meant to serve as examples; they can be enhanced as needed or replaced by other measures capable of providing strong protection. In other words, you will only need to review these requirements if they have been incorporated into your IT-Grundschutz model as a result of a risk analysis (meaning they have become part of your security concept). You will learn more about this topic in lesson 7:*Risk analysis.*

Unit 5.2: Preparation and Execution

During an IT-Grundschutz check, you can determine and document the degree to which the individual measures for a given target object have been implemented by conducting interviews with the employees responsible and on-site inspections (of server rooms and configuration settings, for example).

The quality of the results of these interviews and inspections depends in part on solid preparation and the observation of a number of rules in carrying them out:

- The first and most important rule is that information technology is constantly evolving, which necessitates regular reviews of whether the security measures implemented are still providing adequate protection. This is also why the IT-Grundschutz Compendium is continually adjusted and expanded to include new modules. For your IT-Grundschutz check, please use the **current version of the IT-Grundschutz Compendium**, which is the only version that supports a level of security commensurate with the current state of the art.

- The **documents** that are already available on security-relevant processes, regulations, and circumstances contain a great deal of information that can aid you in determining the extent to which requirements are met. You should thus read through them before proceeding.
- Choose **appropriate contact persons**. Here, you should also decide whether external entities should be involved (third-party companies to which sub-tasks in your information network are delegated, for example). Contacts can be derived directly from the roles cited in each module and from the context at hand. Employees in HR or user support can be good contacts for the *Personnel* module, for example, while the administrators responsible can be helpful sources of information regarding the system modules for networks, IT systems, and applications.
- Four eyes and ears see and hear more than two, so try to conduct interviews **with another person** whenever possible. In these situations, it is a good idea to have one of you lead the conversation and ask the questions while the other documents your findings.
- You should, of course, be familiar with the content of the requirement descriptions and the respective implementation recommendations. In some cases, **summaries** that cover the main aspects of individual requirements and potential measures through which they can be fulfilled can be helpful.
- Finally, another obvious note: An IT-Grundschutz check is a chance to improve information security, not an interrogation. Be sure to provide for a **relaxed atmosphere** during both your conversations and your on-site inspections.

Unit 5.3: Documentation

You can document the **degree of fulfilment** of the IT-Grundschutz requirements pertaining to the various target objects in your information network using the following categories:

- **Unnecessary**: It is not necessary to meet the requirement in question because alternative measures provide at least the same amount of protection against potential threats (password rules are not required when chip cards are also used for authentication purposes, for example) or the recommendations for the purpose under review are not relevant (e.g. the need to secure remote maintenance activities is only important when system maintenance is actually performed from remote locations).
- **Yes**: The requirement in question is fully covered by appropriate and effective measures.
- **Partially**: The requirement in question is only partially fulfilled.
- **No**: The requirement in question has not been met; appropriate measures have largely not been implemented.

The following figure illustrates the corresponding decision-making process:

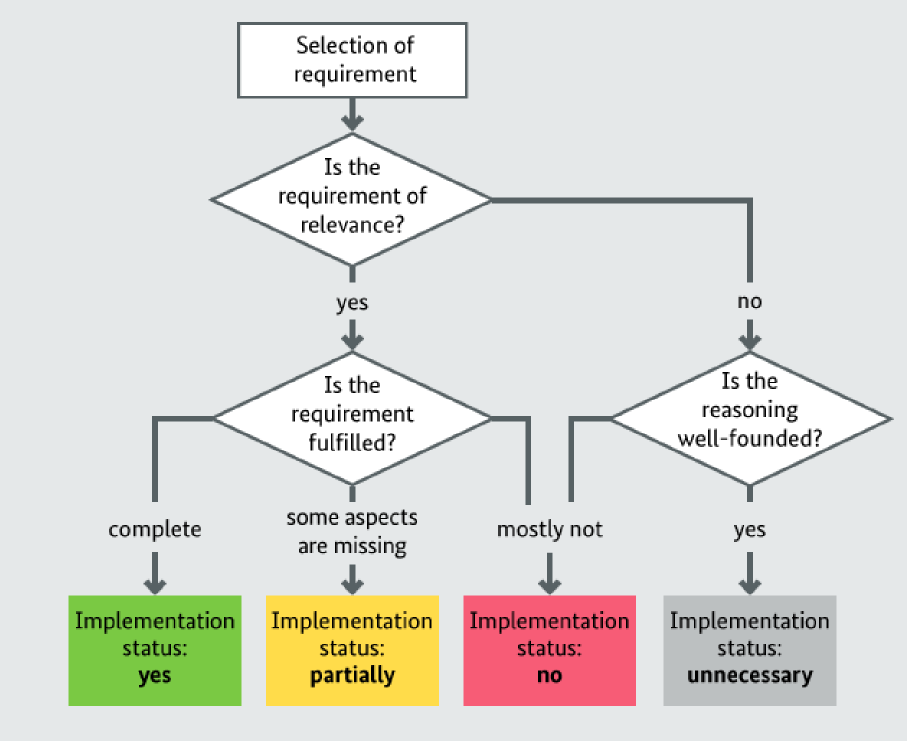

Selection of requirement
Is the requirement of relevance?
yes
no
Is the requirement fulfilled?
Is the reasoning well-founded?
complete
some aspects are missing
mostly not
yes
Implementation status: yes
Implementation status: partially
Implementation status: no
Implementation status: unnecessary

Illustration 12: The decision process for IT-Grundschutz checks

Please note: If a requirement's fulfilment is classified as "unnecessary" due to alternative measures, you must provide evidence that these measures adequately minimise the risks at hand. To this end, you can use the cross-reference table of the respective module to identify the corresponding elementary threats. If alternative measures have been taken, state that they adequately reduce the risk posed by the relevant threats. As a general rule, risks cannot be accepted based on the non-fulfilment of basic requirements. In addition, requirements cannot be classified more or less automatically as "unnecessary" through the general acceptance or exclusion of an elementary threat.

Documentation

To enable others to comprehend and review the results of an IT-Grundschutz check at a later point in time, it is important that you document them thoroughly. For requirements you have classified as unnecessary or partially or entirely unfulfilled, do not forget to include your corresponding **rationale** in your documentation.

Documentation also involves **formal specifications**, of course. For each interview, indicate the following:

- The target object in question
- When the interview took place
- Who conducted it
- Who was interviewed

Resources

A number of resources can facilitate the process of documenting an IT-Grundschutz check:

- The IT-Grundschutz resources include corresponding checklists for all the modules (download here).

- IT-Grundschutz checks are also supported by a series of tools that are tailored to the IT-Grundschutz methodology. Using one of these tools gives you the added benefit of knowing that your structural analysis data will be copied over to the documentation of your IT-Grundschutz check in a consistent manner.

Both the forms included in the IT-Grundschutz resources and the screens in the IT-Grundschutz tools offer fields into which you can enter information on the implementation of measures that have been identified as missing (deadlines, persons responsible, estimated costs, etc). Such details are important for the planning of said implementation. It is not yet necessary to fill these fields out during an IT-Grundschutz check.

Unit 5.4: Decision Criteria

The requirements presented below from the process module ISMS.1 Security management and the system module SYS.2.1 General client are meant to serve as examples of the decision-making process regarding the status of a requirement.

Assessed as "fully implemented"

Among other requirements, the module ISMS.1 contains ISMS.A1: *Acceptance of Overall Responsibility for Information Security at the Executive Level*, which in turn includes six sub-requirements marked as mandatory by the verb MUST:

"The executive level MUST accept overall responsibility for information security within the organisation in a manner clearly recognisable to all those involved. The executive level at the organisation MUST initiate, control, and monitor the security process. The management level MUST exemplify information security.
The top management of the government agency or company MUST appoint the employees responsible for information security and provide them with the necessary authorities and resources. The executive level MUST be informed regularly of the organisation's information security status, and in particular of possible risks and consequences pertaining to security measures that have not been taken."

Assessed as "unnecessary"

In some situations (such as when an organisation lacks sufficient in-house expertise), it can make sense to delegate security tasks to an external information security officer. However, this does not absolve an organisation from its fundamental responsibilities regarding information security. The rights and obligations of an external ISO should thus be defined and established in a contract before proceeding. This basic requirement is specified further in *ISMS.1.A5 Contract Formulation When Appointing an External Information Security Officer*. If the role of ISO is performed by an in-house employee, this requirement obviously does not apply.

Assessed as "partially fulfilled"

The module SYS.2.1 General client, the use of which is mandatory for every group of clients in a given information network, includes the basic requirement SYS.2.1.A2: *Separation of roles*, along with specifications regarding the limitation of users' rights. This requirement states the following:

"The client MUST be configured in such a way that normal activities are not carried out with administrator rights. Only administrators MUST obtain administrator rights. Only administrators MAY change the system configuration, install or remove applications, or modify or delete system files. Users MUST only have read access to system files.
Procedures, framework conditions, requirements for administrative tasks, and the separation of duties among the different roles in the IT system users SHOULD be established in a user and administration concept.

If the fulfilment of this requirement is checked for a given group of clients and it is determined that the IT systems in question are configured to allow common user activities to be carried out only with limited corresponding rights (and that system access is reserved for administrators), at least part of the requirement has been met. The fact that the systems lack an explicit user and administration concept without a pertinent reason is what leads to this requirement's classification as only partially fulfilled.

Assessed as “not fulfilled”

The requirement SYS.2.1.A2: *Separation of roles* (which is part of the module SYS.2.1 General client), on the other hand, is not fulfilled if the aforementioned concept is in place, but only reflects the specifications of this basic requirement to a limited degree – especially if the clients checked deviate significantly from the mandatory requirements at hand.

There can be valid reasons why users should be able to use certain IT systems with administrative rights even though they do not typically have such rights (if special software they require would otherwise not function properly, for example). In such cases, the risk that arises from the non-fulfilment of this basic requirement must be mitigated by additional measures.

Unit 5.5: Example

To offer an example of how an IT-Grundschutz check can be documented, the following excerpt of a check carried out at RECPLAST GmbH presents the results found for three basic requirements and one standard requirement of the module ISMS.1 *Security management.* This module is to be applied to the entire information network at hand – in this case, to the entire company.

For detailed documentation of the IT-Grundschutz check for this module (and other select modules), please refer to chapter 6 of the example document.

Requirement	Responsibility	Status	Implementation
ISMS.1.A1: Acceptance of Overall Responsibility for Information Security at the Executive Level	Organisation management	Fulfilled	The company's executives initiated the creation of an information security policy and signed off on the policy developed. These executives have taken overall responsibility for the subject of information security and delegated the implementation of the measures required to the company's ISO. Once per month, the executives receive a management report, review the current status of the measures being implemented, initiate further actions as required, and approve corresponding budgets.
ISMS.1.A5 Contract Formulation When Appointing an External Information Security Officer	Organisation management	Unnecessary	The information security officer at RECPLAST GmbH is an internal employee.
ISMS.1.A7 Definition of Security Measures	ISO	Partially fulfilled	All the employees involved in implementing measures related to information security are obligated to document them and inform the ISO by e-mail. The measures implemented are neither evaluated nor sufficiently documented. Detailed documentation of these measures is to be implemented by 30 April.
ISMS.1.A11 Information security continuity	ISO	Fulfilled	All documents and processes undergo an internal audit once each year. To this end, the ISO has the corresponding technical authority to issue instructions to employees who are responsible for certain documents and processes.

Table 13: Example documentation of an IT-Grundschutz check

Unit 5.6: Test questions

If you wish, you can use the following questions to test your knowledge regarding IT-Grundschutz checks. See the attachment for solutions to the questions. Please note that multiple answers may be correct.

1 **Which statements regarding IT-Grundschutz checks are correct?**

a An IT-Grundschutz check makes it possible to identify areas in which security requirements have not been met.

b An IT-Grundschutz check only covers the fulfilment of basic requirements.

c An IT-Grundschutz check serves to identify security problems that must then be examined in greater detail in a risk analysis.

d An IT-Grundschutz check compares security requirements against the security measures that have actually been implemented.

2 **What preparations does an IT-Grundschutz check require?**

a A schedule must be set.

b Appropriate interview partners must be selected.

c A penetration test must be carried out to identify vulnerabilities that will be discussed with the interview partners chosen.

d Available documents on information security in the information network under review must be collected and read.

3 **What procedures should you follow to determine how well a group of clients is protected during an IT-Grundschutz check?**

a You should conduct interviews with the system administrators responsible.

b In a penetration test, you should attempt to identify vulnerabilities in the IT systems in question while incorporating all the clients belonging to the group.

c You should perform on-site examinations of random clients and their configurations.

d You should read available documentation on the clients' configurations.

4 **When should you assess a requirement of a given IT-Grundschutz module as fulfilled during an IT-Grundschutz check?**

a When the requirement is fully covered by appropriate and effective measures

b When the corresponding interview partner has given you credible assurances that there have not been any security issues with the IT system in question thus far

c When there is extensive documentation on the protective measures that have been implemented for the IT system in question

d When neither random checking nor the interview conducted with the person responsible for the IT system has revealed any security flaws

5 **How should you proceed in dealing with specifications for higher protection requirements during a first-time IT-Grundschutz check (that is, before carrying out risk analyses)?**

a As a rule, you should classify these specifications as unnecessary and also forgo checking them once they have been implemented at your organisation.

b You should remove these specifications from your target concept.

c You should examine the specifications for high and very high protection requirements only after your risk analysis is complete.

d As a rule, you should examine all the specifications cited in the IT-Grundschutz modules during an IT-Grundschutz check, including those pertaining to higher protection requirements.

6 **You discover that a standard requirement has not been met for an IT system that will soon be decommissioned. How should you treat this requirement in an IT-Grundschutz check?**

a You should remove the requirement from your IT-Grundschutz model.

b You should document the requirement as unnecessary, as fulfilling it would no longer be cost-efficient.

c You should document the requirement as not fulfilled and consider including a note that measures meant to address this shortcoming should be reviewed in terms of their cost-efficiency due to the impending decommissioning of the IT system in question.

d You should document the requirement as not fulfilled and include a note that the resulting risks should be reviewed in terms of whether they are acceptable due to the impending decommissioning of the IT system in question.

Lesson 6: Risk analysis

The production strongly depends on this server!
In this case, we may have to do more!
SOFT DRINKS

The manner in which the basic and standard requirements of the IT-Grundschutz modules have been established is meant to result in measures that are suitable for **normal protection requirements** and capable of providing adequate protection for **typical information networks and application scenarios**. To this end, an advance effort was made to identify the threats that are commonly present in the situations covered in the modules and determine how the resulting risks can be effectively addressed. This means that as you apply IT-Grundschutz, you will typically not need to perform any further extensive analyses to identify the security measures necessary in all but a few areas of the information network at hand.

Additional analyses are only required in the following three cases:

- A target object has high or very high protection requirements regarding at least one of the three basic values (confidentiality, integrity, and availability).
- The IT-Grundschutz Compendium contains no sufficiently applicable module for a given target object.
- A suitable module is available for a given target object, but the environment in which it is used is atypical from an IT-Grundschutz perspective.
- In this context, a **risk analysis** is the fundamental approach to examining security threats and their ramifications. BSI Standard 200-3: *Risk Management* offers an efficient methodology for such purposes.

In this lesson, you will gain an in-depth understanding of **how to perform a risk analysis in line with BSI Standard 200-3**. In particular, it covers the following:

- The prerequisites that should be met before carrying out risk analyses at your organisation
- How to use the list of elementary threats in the IT-Grundschutz Compendium to compile a threat overview for a given target object
- How to identify and assess the risks presented by these threats
- How to take effective decisions on how to address risks
- How to incorporate the results of risk analyses back into your security process

Unit 6.1: Organisational Framework Conditions

Before you start carrying out risk analyses, your organisation's executives should establish some basic related aspects in a **guideline for dealing with risks**.

- Under what circumstances is a risk analysis necessary?
- What procedure should be followed to identify, assess, and address risks; how is it tailored to the circumstances at your organisation; and how is it integrated into your security process?
- Which organisational units are responsible for the various sub-tasks involved in risk management?
- How have the related reporting obligations been defined?
- What criteria do risks need to fulfil in order to be acceptable?
- How frequently and after what events do risk analyses need to be updated?

A guideline of this kind and the organisational measures taken should be reviewed in terms of their currentness and suitability on a regular basis.

Example: risk management at RECPLAST GmbH

RECPLAST GmbH has decided to align its risk management with IT-Grundschutz and develop a security concept based around the Standard Protection. For objects with normal protection requirements, the company handles risks with the help of the basic and standard requirements found in the IT-Grundschutz Compendium. It has established BSI Standard 200-3 as its method for performing any risk analyses that prove necessary. In its guideline for dealing with risks, RECPLAST has also stipulated that risks resulting from a failure to fulfil basic requirements cannot be accepted. In addition, risks should be addressed under consideration of the costs of the potential measures involved and their effectiveness in minimising said risks.

The person responsible for performing risk analyses is the company's ISO, who assembles specialised teams for this purpose. The members are assigned based on the situation at hand: Those responsible for applications help assess the potential ramifications of damage, for example, while specialised employees from IT are brought in to evaluate risks that require a high level of technical expertise.

The risk analyses carried out are documented, and their results are presented to the company's executives along with corresponding suggestions on how to deal with the risks at hand for subsequent coordination. Annual reviews are to be conducted to ensure that risk analyses are still current and appropriate.

How does your company or government agency approach this subject? Is there a defined process for identifying, assessing, and dealing with information security risks? Are risk analyses conducted at your organisation, and if so, what procedure is followed? Who is responsible for performing these analyses? Who receives the results, and how are related conclusions drawn?

Unit 6.2: Assembling Target Objects

In order to carry out risk analyses in the context of implementing the Standard Protection, the target objects of the information network in question must first be documented during structural analysis. Their protection requirements then need to be determined, and the objects must be assigned suitable IT-Grundschutz modules to the greatest extent possible during modelling.

At the beginning of this lesson, you learned that a risk analysis should be performed on the following target objects:

- Those that have high or very high protection requirements regarding at least one of the three basic values (confidentiality, integrity, availability)
- Those for which none of the IT-Grundschutz modules are appropriate
- Those operated in scenarios that are atypical from an IT-Grundschutz perspective

If you have a **large number of target objects** that meet one of these criteria, you should find an **appropriate means of prioritising them**. When implementing the Standard Protection, it is helpful to start by examining overarching target objects, such as the entire information network, specific components thereof, or key business processes. When implementing the Core Protection, you should give priority to the target objects with the highest protection requirements.

Example

At RECPLAST GmbH, the processes of determining protection requirements and modelling identified a series of target objects for which a risk analysis needs to be conducted. These objects include the following:

- The application A007 *Lotus Notes*, which has high confidentiality requirements and very high availability requirements
- The network coupling elements N001 *Internet Connection Router* and N002 *Internet Access Firewall* due to the confidentiality of the data they are used to transmit
- The virtualisation server S020, which has high protection requirements regarding all three basic values due to the virtual systems it runs
- The alarm systems S200 and S201 at the company's two locations in Bonn, whose proper functionality has been classified as crucial; its protection requirements in terms of integrity and availability have thus been assessed as “very high”
- Taking the virtualisation server S020 (which is designed for redundancy across RECPLAST’s two locations) as an example, the individual steps involved in risk analysis are covered below.

Unit 6.3: Elementary Threats

To provide a key resource for conducting risk analyses, the IT-Grundschutz Compendium contains a list of **47 elementary threats** that is compatible with comparable lists used by various international standards and norms.

The individual threats are differentiated by means of unique identifiers and descriptors. Each threat also comes with a brief description that is designed to be as product- and technology-agnostic as possible, as well as an indication of which of the basic values (confidentiality, availability, integrity) could be directly affected.

The following selection illustrates the broad spectrum of threats and damage scenarios covered. It ranges from technical failures and force majeure to organisational flaws and people's negligent or deliberately improper behaviour. The basic values impacted in each case are indicated by the letters “C” (confidentiality), “I” (integrity), and “A” (availability).

Threat	Basic value(s) affected
G 0.1 *Fire*	A
G 0.5 *Natural catastrophes*	A
G 0.10 *Failure or malfunction of supply networks*	A
G 0.15 *Line tapping*	C

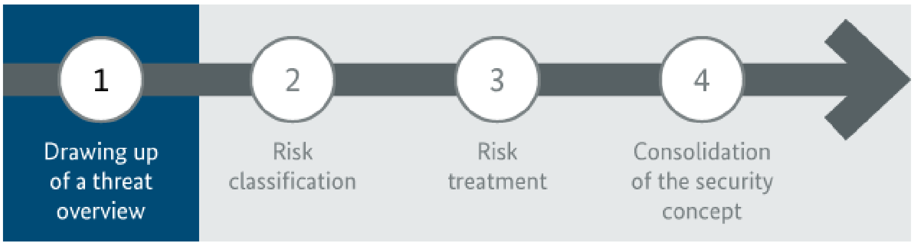
Threat	Basic value(s) affected
G 0.18 Poor planning or lack of adjustment	C, I, A
G 0.23 *Unauthorised entry into IT systems*	C, I
G 0.26 *Malfunctions of devices or systems*	C, I, A
G 0.31 *Incorrect use or administration of devices and systems*	C, I, A
G 0.33 Loss of personnel	A
G 0.39 *Malware*	C, I, A
G 0.46 *Loss of integrity of information that should be protected*	I

Table 14: Examples of elementary threats

The requirements formulated in the IT-Grundschutz modules have been compiled under consideration of the elementary threats relevant in each case. This is why the final section of each module includes a matrix that maps the relationships among the requirements and elementary threats at hand.

In the next unit, you will learn how to use elementary threats for your own risk analyses.

Unit 6.4: Creating a Threat Overview


1
Drawing up of a threat overview
2
Risk classification
3
Risk treatment
4
Consolidation of the security concept

The first step of risk analysis is to identify the risks to which a given object or situation is exposed. You should begin by describing the threats that can potentially impact the object or situation.

In line with BSI Standard 200-3, you can use the **elementary threats as a starting point**. It is important to differentiate between two cases in this context:

- **A suitable module for the target object in question does not (yet) exist.** In this case, you can consult the full list of elementary threats and check which of them are relevant to the target object.
- **There is a suitable module for the target object.**

In this case, a risk analysis has already been conducted for the type of target object at hand. The modules contain a tabular presentation that indicates which elementary threats are relevant and what requirements have been defined to address them. Your job is to check whether any other elementary threats could lead to significant damage.

You should determine the relevance of a threat based on its potential impact. In doing so, it is important to distinguish between threats that directly affect the object in question and those that have an indirect impact through other, more general threats. You should only incorporate threats with direct relevance into your threat overview.

Example

Based on previous modelling, the following three IT-Grundschutz modules are relevant to the virtualisation server S020: SYS.1.1 *General server*, SYS.1.3 Servers under Unix, and SYS.1.5

Virtualisation. The following overview of relevant threats (which is not presented in full) can thus be assembled from the elementary threats referenced in these modules:

- G 0.14 *Espionage*
- G 0.15 *Line tapping*
- G 0.18 Poor planning or lack of adjustment
- G 0.19 *Disclosure of information that should be protected*
- G 0.21 *Manipulation of hardware or software*
- G 0.22 *Manipulation of information*
- G 0.23 *Unauthorised entry into IT systems*
- G 0.25 *Failure of devices or systems*
- G 0.26 *Malfunctions of devices or systems*
- G 0.28 *Software vulnerabilities or errors*
- G 0.30 *Unauthorised use or administration of devices and systems*
- G 0.31 *Incorrect use or administration of devices and systems*
- G 0.32 *Misuse of authorisations*
- G 0.40 *Denial of services*
- G 0.43 *Importing of messages*
- G 0.45 Loss of data
- *G 0.46 Loss of integrity of information that should be protected*

Unit 6.5: Completing a Threat Overview

Although the list of elementary threats covers a wide range of dangers to which information and IT are exposed, the presence of other threats requiring your attention cannot be ruled out. This is particularly relevant when a given target object is operated in atypical scenarios.

To follow up on the first step in creating a threat overview, you should thus check whether there are other hazards to examine along with the applicable elementary threats.

How can you identify additional threats?

One proven way to identify potential threats involves having your ISO or another security expert hold a moderated workshop for employees who deal with the component in question in some way (such as users, administrators, or those in application support). Manufacturer documentation and online publications can also serve as sources of tips on possible threats.

The elementary threats were chosen in such a way that they provide a compact, adequate and, in typical scenarios, complete basis for risk analyses. For this reason, the focus, when determining additional threats, should not be to identify additional elementary threats. However, it can make sense to consider specific aspects of an elementary threat, as this may make it easier to identify specific safeguards.

What should you keep in mind?
In some instances, the aforementioned workshop can present an opportunity to discuss many different types of threats. To avoid making the subsequent assessment of these threats more difficult than necessary, you should:

- Concentrate on the threats that have a negative impact on the basic values for which the target object in question has high or very high protection requirements
- Factor in all the areas into which the threat catalogues are grouped – that is, force majeure, organisational flaws, human error, technical failures, and malicious attacks by internal and external perpetrators – and group the threats in question accordingly
- Consider the relevance of the suggestions made and only pursue threats that could lead to significant damage and are realistic in the context at hand
- For every suggestion made, check whether the corresponding threat is already covered by another threat you have already taken into account
- Generalise the remaining suggestions to reduce the number of threats you will need to cover in the subsequent steps

Like the other steps involved in risk analysis, identifying threats requires in-depth expertise. Publicly accessible information such as magazine articles and online resources can provide valuable tips in many cases. Consulting external experts for advice is often a good idea, as well.

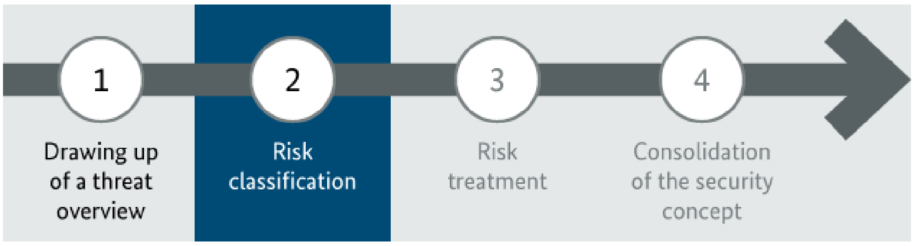
Example

A discussion of other risks to be considered at RECPLAST GmbH results in the decision to treat possible manipulation by family members and visitors as an additional threat to the entire information network at hand due to the frequent presence of such individuals. The threat is described as follows:

> T z.1 *Manipulation by Family Members or Visitors*
> Family members and visitors have temporarily access to certain premises of the company. There is the risk that these persons use this opportunity to make unauthorised changes to the hardware, software or information. This additional threat is a more specific form of the elementary threats G 0.21 *Manipulation of hardware or software* and G 0.22 *Manipulation of information*.

Other additional threats have also been identified, including damage that could be caused to IT in production due to the special characteristics of such environments (dust, vibration, and so on). In risk analyses regarding ICS components, this threat is to be associated with high or very high protection requirements.

Unit 6.6: Assessing Frequency and Ramifications


1
Drawing up of a threat overview
2
Risk classification
3
Risk treatment
4
Consolidation of the security concept

The significance of a given risk is derived from the frequency of a corresponding **threat** and the **amount of damage** it could cause. The more frequently a threat occurs, the greater the risk it presents; by the same token, a risk capable of causing less damage is not as significant.

Generally speaking, the two sides of the equation can be defined in both **quantitative** (that is, with exact numerical values) and **qualitative** terms (categories that describe the degree at hand). Experience has shown, however, that sufficiently reliable quantitative specifications (particularly regarding the frequency of damage events pertaining to information security) essentially do not exist; even in cases where reliable statistics are available, using them to derive exact forecasts of future events is problematic, if not impossible. As in the context of determining protection requirements, a **qualitative approach involving a limited number of categories** is thus advisable.

> The number and definitions of the categories you use to describe how often events occur and how much damage they cause should be tailored to the circumstances your organisation deals with in practice. As a rule, no more than five levels are necessary to differentiate among different degrees of frequency and ramifications. If an overarching risk management approach is already in place at your organisation, it is also a good idea to use the same systems to assess and classify the information security risks you encounter.

The following example of a four-level scheme that could be used to classify frequency of occurrence is based on a suggestion in BSI Standard 200-3:

Frequency of occurrence	Description
Rarely	Based on the organisation's current knowledge, the event can occur every five years at most.
Medium	The event occurs between once every five years to once a year.
Frequently	The event occurs between once a year and once a month.
Very frequent	The event occurs several times a month.

Table 15: Example of how to classify frequency

BSI Standard 200-3 also includes an example of a four-level scheme for classifying the potential damage that could be caused.

Level of damage	Ramifications of damage
Negligible	The effects of damage are low and can be neglected.
Limited	The effects of the damage are limited and manageable.
Considerable	The effects of damage can be considerable.
Threatening the existence of the organisation	The effects of the damage may be so catastrophic that they threaten the organisation's very existence.

Table 16: Example of how to classify the ramifications of damage

> When defining categories to assess a threat’s ramifications, be sure to factor in the categories of protection requirements that have been defined at your organisation. These two systems should be established in such a way that their definitions correspond.

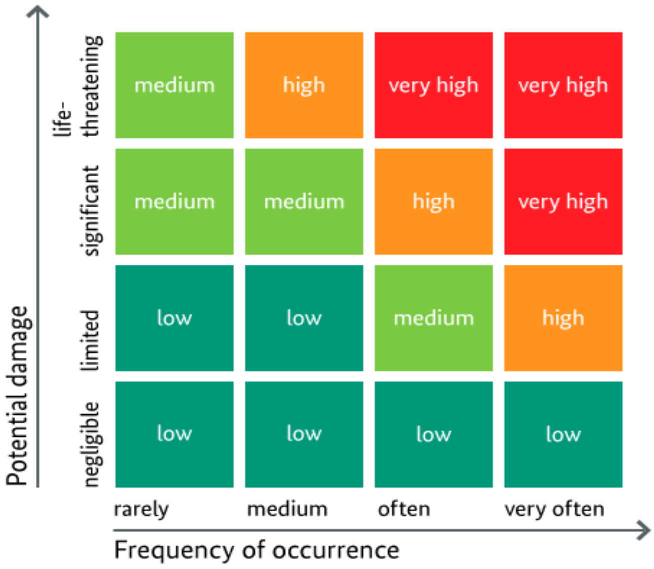
Unit 6.7: Assessing Risks

Once you have evaluated the frequency with which a threat occurs and the damage it can cause, you can assess the amount of risk posed by the combination of these two factors. This is another area where you should avoid using too many **categories**; three to five are common, and just two are used in many cases. BSI Standard 200-3 provides an example with four levels that you can adapt to the circumstances and requirements of your organisation. The following table is based on said example:

Risk category	Definition
Low	The measures already implemented (or at least envisaged) in the organisation's security concept provide adequate protection.
Medium	The measures already implemented (or at least envisaged) in the security concept may not be sufficient.
High	The measures already implemented (or at least envisaged) in the security concept do not offer sufficient protection against the threat in question. It is highly likely that the risk cannot be accepted.
Very high	The measures already implemented (or at least envisaged) in the security concept do not provide adequate protection against the threat in question. It is almost certain that the risk cannot be accepted.

Table 17: Example of how to classify risks

A risk matrix is a common and highly illustrative instrument that can be used to present risks in terms of their frequency of occurrence and the damage they can cause. BSI Standard 200-3 also contains a suggestion you can adapt to the provisions your organisation has made with regard to risk assessment.



Potential damage	rarely	medium	often	very often
life-threatening	medium	high	very high	very high
significant	medium	medium	high	very high
limited	low	low	medium	high
negligible	low	low	low	low

Illustration 13: Example of a risk matrix

Assessing risks enables you to take well-founded decisions on how to deal with potential threats. You may have to decide what additional measures to take to reduce the frequency and/or ramifications of a threat, for example. Using a corresponding matrix, you can also illustrate how implementing such measures would impact a given risk.

Unit 6.8: Example of risk assessment

As an example of risk assessment, let us consider two threats to which the virtualisation server S020 is exposed at RECPLAST GmbH. The corresponding risks are to be assessed based on the aforementioned categories of frequency and ramifications.

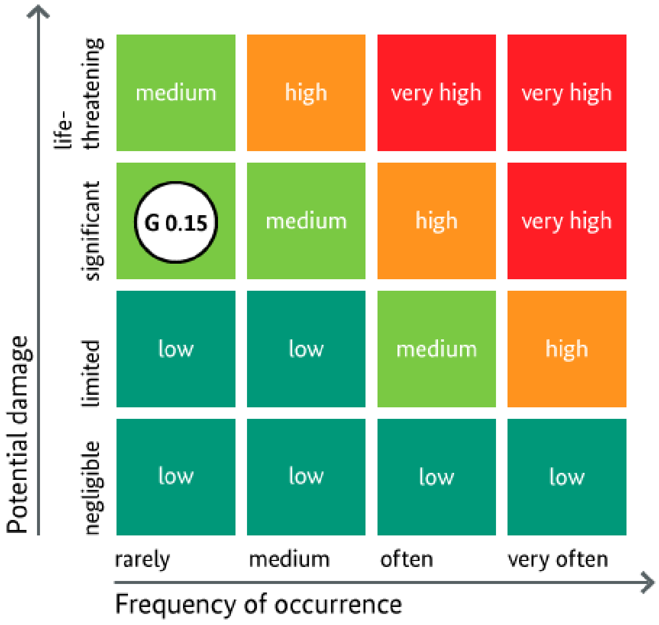
Risk assessment regarding threat G 0.15, Line tapping

This risk arises from the fact that the virtual machines run on server S020 are shifted to a second virtualisation server from time to time for maintenance purposes. During the live migration involved, the current contents of the virtual machines are transferred between the two servers. Since the decision was made not to encrypt these data due to the impact it would have on performance, the information transferred could theoretically be accessed by another party. The same applies to data transferred from virtualisation server S1 to the central storage systems to which it is connected.

In assessing this risk, its frequency of occurrence and the potential ramifications are taken into account:

- The **frequency of occurrence** is determined to be rare, even when no additional measures are taken. This decision was taken because appropriate network segmentation and configuration ensure that when data are transferred during live migration and to the company's storage systems, this takes place in separate sub-networks that are not externally accessible. Access is also limited to authorised administrators who have been deemed trustworthy.
- That said, the data transferred are of a nature that could result in significant negative consequences should their confidentiality be violated. The **ramifications** of this **threat** occurring are thus classified as “considerable”.

Based on the criteria defined for risk assessment, these appraisals indicate that the threat presents a **moderate risk**.



	rarely	medium	often	very often
life-threatening	medium	high	very high	very high
significant	G 0.15	medium	high	very high
limited	low	low	medium	high
negligible	low	low	low	low

Illustration 14: Risk matrix depicting an assessed threat

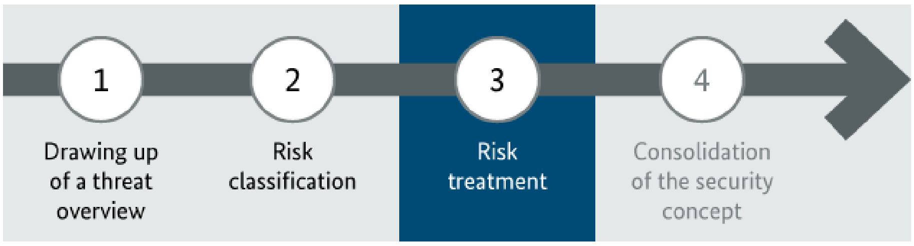
Risk assessment regarding threat G 0.25, Failure of devices or systems

Chapter 5.2 of BSI Standard 200-3 contains various examples of how a risk assessment can be documented in a tabular format. Since it is often the case that a large number of threats need to be considered, it is not necessary to provide detailed explanations of the assessments rendered. The following table provides an example of sufficient risk assessment documentation based on threat G 0.25:

Virtualisation Server S020 **Confidentiality: high** **Integrity: high** **Availability: high**		
Threat G 0.25 *Failure of devices or systems*	Core values impaired: Availability	
Frequency of occurrence without additional safeguards: Medium	Effects without additional safeguards: Considerable	Risk without additional safeguards: **moderate**

Table 18: Example of tabular documentation of risk analysis

Unit 6.9: Addressing Risks


1
Drawing up of a threat overview
2
Risk classification
3
Risk treatment
4
Consolidation of the security concept

Most of the time, threat assessment will reveal that not all the threats present are adequately covered by the security concept in place. In such cases, you will need to consider appropriate ways to deal with these remaining threats and make a sound decision as to which approach is best.

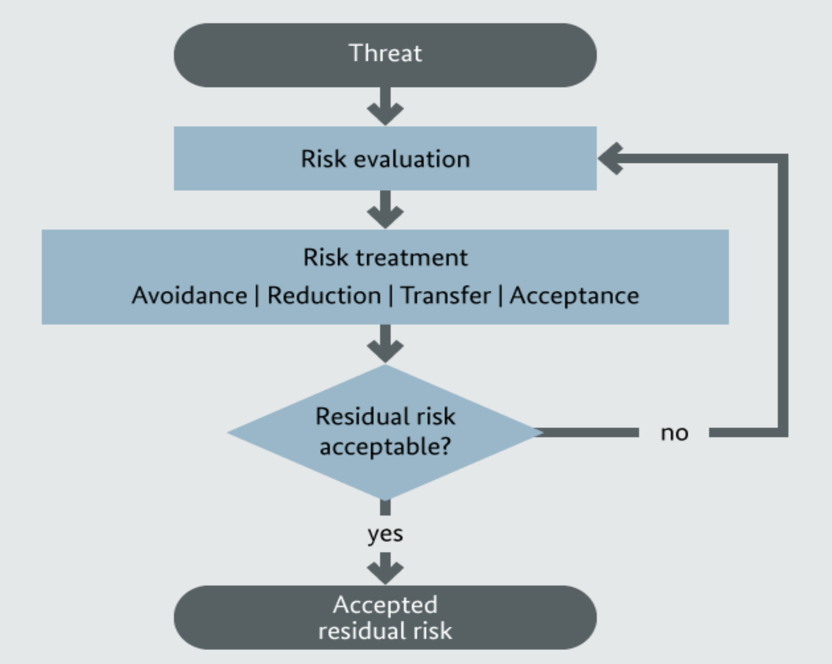

Threat
Risk evaluation
Risk treatment
Avoidance | Reduction | Transfer | Acceptance
Residual risk acceptable?
no
yes
Accepted residual risk

Illustration 15: Addressing risks

In general terms, it is possible to differentiate between four **options** in dealing with risks:

- **A: Avoid risk by restructuring business processes**
  Risks can be avoided by restructuring the information network at hand in a manner that neutralises the respective threats. This may be appropriate when a given risk is not acceptable and while countermeasures are possible, they would entail an inordinate amount of resources.
- **B: Risk reduction (modification) through additional security measures**
  Risks can be mitigated by additional, more effective security measures. If a module is already available in the IT-Grundschutz Compendium for the target object you examined during risk analysis, the specifications it cites for increased protection requirements will include corresponding implementation recommendations and some initial tips on suitable measures. Product documentation, information security standards, and specialised publications offer further resources on this topic.
- **C: Risk transfer**
  Risks can be passed on to another entity. By taking out corresponding insurance policies or outsourcing high-risk activities to an external service provider, for example, it is possible to shift at least part of a potential financial loss to third parties. If you choose this approach, be sure that your corresponding contracts are formulated in a clear and proper manner!
- **D: Risk acceptance**
  Risks can simply be accepted for a number of reasons: A threat could only cause damage under highly extraordinary circumstances, there may be no known and effective means of counteracting it, or the cost of potential safeguards may be disproportionately high, for example.

A risk can only be accepted when the **residual risk** in question (after safeguards are implemented, for example) corresponds to the risk acceptance criteria in place at the organisation at hand.

Risks subject to monitoring

While some risks may be temporarily acceptable, it can be assumed that the threat situation will change in the future and allow the risks to rise to an unacceptable level. In these instances, it is a good idea to monitor the risks in question and follow up periodically to determine whether action might be needed after all. It also makes sense to prepare appropriate safeguards in advance so that it is possible to implement them in short order once the respective risks are no longer acceptable.

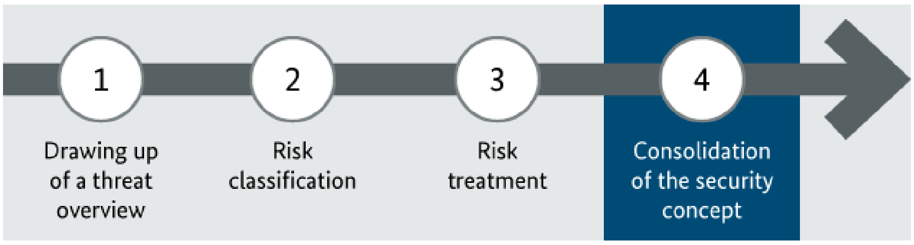
All of an organisation's decisions in this context must have the support of its executives. Management must be willing to bear the costs of reducing or transferring risks, along with the responsibility for any risks accepted This is why you should involve the executive level in related discussions when appropriate. You should also document such decisions in such a way that they can be followed by third parties (auditors, for example) and **have management sign off** on said documentation.

Example

Taking the two threats covered above as an example, the following table lists the decisions taken to address the risks to the virtualisation server at RECPLAST GmbH:

Threat	Risk category	Risk treatment option
G 0.15 *Line tapping* *(In this case, during live migration)*	**Medium**	**D. Risk acceptance** (risk will be accepted without additional safeguards) The live migration network can only be accessed by authorised administrators. They are trusted. The residual risk is deemed acceptable by RECPLAST GmbH.
G 0.25 *Failure of devices or systems* (In this case, failure of the virtualisation server)	**Medium** Mit ergänzenden Maßnahmen: **gering**	**B: Risk reduction** Supplementary safeguard: The server is designed redundantly to ensure that the virtual infrastructure can still be operated without problems in the case of a failure. The system is also configured in such a way that when a failure occurs, the system automatically switches to a backup server within the cluster.

Unit 6.10: Subsequent Steps


1
Drawing up of a threat overview
2
Risk classification
3
Risk treatment
4
Consolidation of the security concept

To complete risk analysis, the additional measures your organisation has decided to implement need to be integrated into your existing security concept (this is also referred to as consolidating the security concept). The security process can then continue on this basis.

Consolidating the security concept

In this step, you should review the **suitability**, **appropriateness**, and **user-friendliness** of your additional measures, along with how they **dovetail** with other measures. This consolidation of your security concept can lead to both adjustments in the additional measures you have selected and changes in the concept.

For more information on consolidating security measures, please refer to Unit 7.1: *Consolidating Measures*.

Continuing the security process

Following the consolidation of your security concept, you can proceed with the subsequent steps in your security process. In particular, this should involve reviewing and documenting the implementation status of the measures you have added or modified in **another IT-Grundschutz check** as described in one of the previous lessons (IT-Grundschutz Check).

> ! A second IT-Grundschutz check is necessary because the security concept at hand usually changes in the course of risk analysis and the implementation status of new and modified measures needs to be reviewed.

Unit 6.11: Test questions

If you wish, you can use the following questions to test your knowledge of risk analysis in accordance with BSI Standard 200-3. See the attachment for solutions to the questions. Please note that multiple answers may be correct.

1 **Who bears responsibility for the decisions taken regarding a given IT system during risk analysis?**

a The IT system's administrator

b The organisation's executives

c The information security officer

d The IS management team

2 **Which threats are examined in the first step of creating a threat overview?**

a The risk catalogues found in the appendix to BSI Standard 200-3

b The relevant elementary threats from the IT-Grundschutz Compendium

c The threats listed in the appendix to the ISO 27005 norm

d The specific threats listed in a module's sections on the threat situation at hand

3 **What should you evaluate when assessing risk?**

a How frequently a threat occurs

b The scale of damage associated with a threat

c The protection objectives impacted by a threat

d The effectiveness of the measures planned and already implemented to address a threat

4 **How can you transfer risk?**

a By taking out an insurance policy

b By outsourcing a high-risk business process to an external service provider

c By restructuring a high-risk business process

d By deciding to take risk-mitigating measures only after the necessary financial resources become available

5 **What reasons may justify accepting a high level of risk?**

a Potential safeguards would require an inordinate amount of resources.

b Similar organisations also accept the risk in question.

c There are no effective safeguards against the risk in question.

d The threat from which the risk stems has not led to a significant security incident thus far.

6 **In principle, when can a risk not be accepted?**

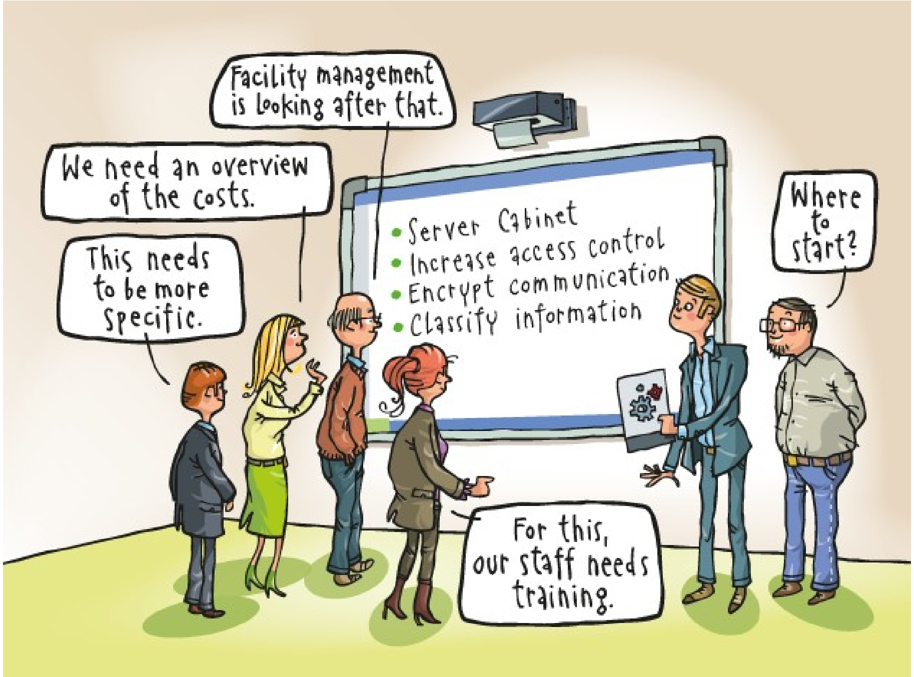
a When basic requirements are not fulfilled

b When elementary threats are present

c When a situation calls for very high protection requirements

d When standard requirements are not fulfilled

Lesson 7: Implementation planning


Facility management is looking after that.
We need an overview of the costs.
This needs to be more specific.
• Server Cabinet
• Increase access control
• Encrypt communication
• Classify information
Where to start?
For this, our staff needs training.

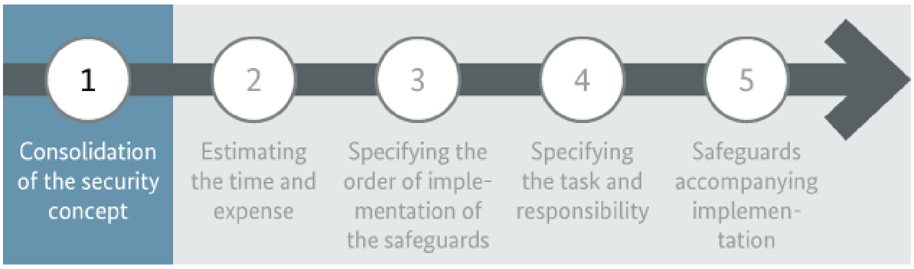
Are all the basic and standard requirements met at your organisation? Have you conducted risk analyses and determined that target objects with special protection requirements are also adequately secured? If so, you have no doubt achieved a solid level of security at your organisation and can now focus on maintaining and improving it.

In most cases, however, an IT-Grundschutz check and additional risk analyses lead to a different outcome: There are always flaws of some kind, whether in your established organisational regulations; the extent to which you monitor them; your security technology; or structural safeguards against fire, water, and theft.

One of the aims of implementation planning is to eliminate such flaws in an efficient and effective manner. In this lesson, you will be introduced to a systematic approach you can follow, particularly when a large number of individual measures need to be implemented. You will learn about:

- The aspects to consider when implementing security measures
- The resources IT-Grundschutz provides to support you in doing so
- What you should do when effective security measures cannot be implemented immediately
- How to document the results of your implementation planning

Unit 7.1: Consolidating Measures


1
Consolidation of the security concept
2
Estimating the time and expense
3
Specifying the order of imple-mentation of the safeguards
4
Specifying the task and responsibility
5
Safeguards accompanying implemen-tation

The **first step** involves filtering requirements that are **not or only partially met** out of the results of the IT-Grundschutz check and any risk analyses you have conducted.

To produce clear documentation, you should **make a tabular list** of the requirements that are not sufficiently met and group them by the target objects affected (the entire information network, for example, or specific IT systems and physical spaces).

You can then define the **measures** with which you will close these security gaps. Here, the implementation recommendations for the individual IT-Grundschutz modules are available as a related resource.

In the next step, you will examine how the measures **interrelate** while checking the following:

- Whether specific measures will be made redundant by other measures that will provide at least the same level of protection for the respective target object
- Which measures still need to be specified in detail and adapted to the particular circumstances of your organisation
- Whether the measures are actually suitable and appropriate – do they provide adequate protection without hindering workflows or impairing the effectiveness of other security measures?

The objective here is to eliminate redundant measures and flesh out the details of those that remain in order to reduce the financial and personnel resources required to the necessary minimum.

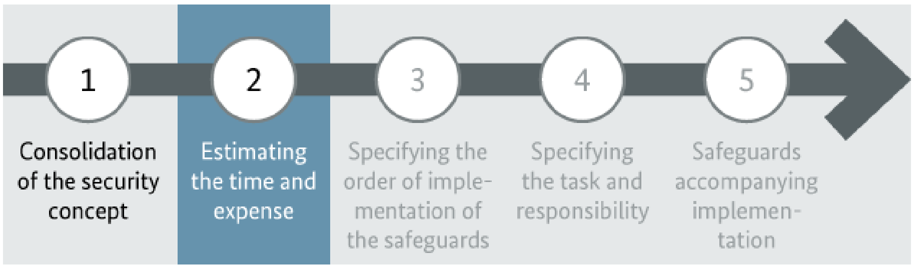
When this step is complete, you will have a list of specific measures that are tailored to your particular organisation. To make it easier to follow the decisions you take in comparing and adjusting measures, be sure to document the rationale behind them.

Examples

These examples are meant to illustrate the questions that can arise and possible ways to address them as you consolidate measures.

- If a risk analysis has determined that an authentication procedure based on chip cards or tokens should be implemented for a group of IT systems, measures designed to ensure highly complex passwords may no longer be necessary.
- Mistakes in building planning can often only be corrected with a disproportionate amount of resources after the fact. If certain requirements (regarding the avoidance of water lines in specific areas, for instance) cannot be fully met in a cost-efficient manner due to the structural circumstances at hand, alternative measures should at least be taken. These might include installing troughs below the water lines to catch and divert any leaks, along with a water alarm that can be heard in an area constantly occupied by a gatekeeper. This would at least make it possible to identify water damage early on and limit the ramifications.
- In some situations, access control measures could block possible escape routes to be used in case of fire. Here, fire prevention experts (the local fire brigade, for instance) should be consulted in order to find a proper balance between these concerns and those pertaining to facility access.
- Encrypting business-critical information to preserve its confidentiality is an example of a measure that can conflict with other security objectives. This is why it is important to weigh the advantages and drawbacks carefully and take supplementary measures when circumstances warrant them.
  - Encrypted e-mails, for instance, can slip past a server's main antivirus software and infiltrate a network with malicious software.
  - If inadequate provisions are in place to ensure the proper use and management of the keys involved, encryption also comes with the risk that crucial data may become inaccessible to authorised individuals.

Unit 7.2: Estimating Resource Requirements


1
Consolidation of the security concept
2
Estimating the time and expense
3
Specifying the order of imple-mentation of the safeguards
4
Specifying the task and responsibility
5
Safeguards accompanying implemen-tation

In light of the typically limited budgets allocated to information security, it is necessary to compile an overview of the fixed and variable costs expected for each individual measure. The next step thus involves estimating the one-time and recurring costs (in terms of both finances and personnel) that will be required to implement the specific measures planned.

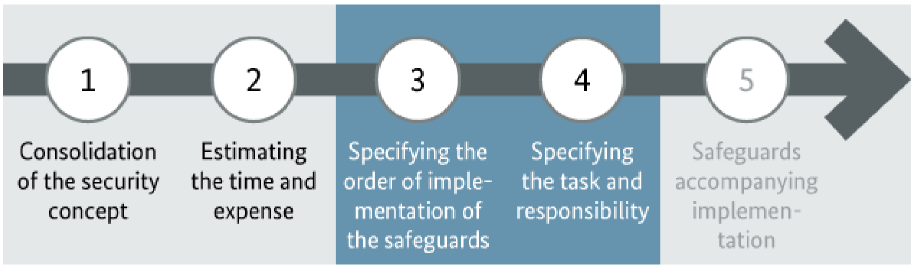
Your organisation's executives must support the use of personnel and finances for these purposes. This is particularly important when the amount of funding approved is not enough to implement all the measures immediately and a decision needs to be taken as to whether to increase the budget or accept the risk inherent in not implementing said measures.

To lay the groundwork for a top-level decision on implementing security measures, you should:

- Develop a proposal on how to distribute the budget
- Consider more affordable alternatives if implementing specific measures would exceed the expected budget
- Make the executives aware of the residual risks inherent in not fulfilling the security requirements at hand; to back up your arguments, you can use the cross-reference tables found at the end of every IT-Grundschutz module, which describe the threats each requirement is designed to address
- Ensure that the executives provide signatures to confirm that they are willing to accept the residual risks at hand in deciding on the budget

Remember that meeting the relevant basic requirements is the minimum level of security necessary in accordance with IT-Grundschutz. For this reason, any risks stemming from a failure to fulfil such requirements should not be accepted.

Unit 7.3: Establishing Order of Implementation and Related Responsibilities


1
Consolidation of the security concept
2
Estimating the time and expense
3
Specifying the order of imple-mentation of the safeguards
4
Specifying the task and responsibility
5
Safeguards accompanying implemen-tation

When the personnel or budget available is not sufficient to implement all the intended security measures immediately, you will need to establish a suitable order of implementation. In doing so, you should focus on the following rules:

- An initial indication of how your order of implementation should be set is provided by the **indicators R1, R2, and R3**, which are found in the modelling recommendations in chapter 2.2 of the IT-Grundschutz Compendium. Requirements from modules labelled “R1” (such as ISMS.1 *Security management* and the modules in the ORP. *Organisation and Personnel* layer) should be fulfilled first. Requirements from “R2” modules should come next, followed by those from “R3” modules.
- In addition, measures designed to fulfil **basic requirements** should generally be implemented first, followed by those that meet **standard requirements** and then those meant to fulfil **higher protection requirements**.
- You should also consider the **logical connections** among the individual measures at hand; those that serve as prerequisites of other measures should be implemented first, for example.

In particular, you will need to keep an eye on how implementing specific measures will impact your information network's overall level of security. Give priority to taking measures that:

- Involve components with higher protection requirements (secure servers before clients, for instance)
- Have a more widespread impact (centralised measures such as the use of network and system management tools)
- Affect areas in which there is a notable lack of security measures

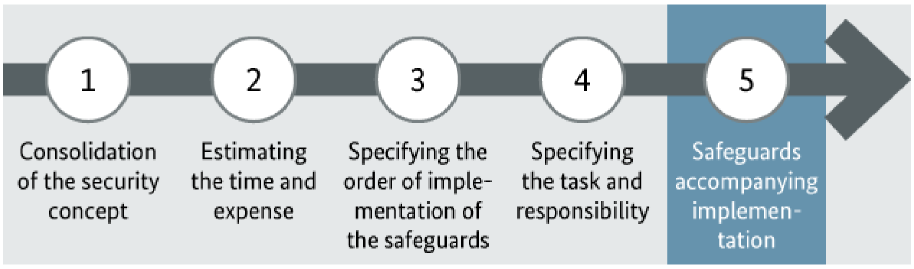
Document your decisions regarding order of implementation and the rationale behind them with care to make sure others can understand why you have accepted the residual risks inherent in implementing certain measures in stages over time. This can be especially important during legal disputes as evidence of due diligence.

Assigning tasks and responsibilities

Measures are usually only implemented on schedule when people are made responsible for ensuring that this occurs by a certain date. The next step thus involves appointing those who will be initiating and carrying out the implementation. These decisions should also be made in coordination with your organisation's executives.

Make sure that those responsible for implementations have sufficient skills and expertise, as well as access to the resources required. You will also need to plan any training courses that prove necessary.

Unit 7.4: Planning Support Measures


1
Consolidation of the security concept
2
Estimating the time and expense
3
Specifying the order of imple-mentation of the safeguards
4
Specifying the task and responsibility
5
Safeguards accompanying implemen-tation

The success of a given measure depends to a large extent on how it is accepted and applied by the employees affected. This is why it is important to ensure that these employees are adequately trained and made aware of potential problems during the implementation of new security measures.

Plan training activities!

Implementing new security measures always entails providing the employees affected with training related to the tasks and products involved. After all, what good is a new fire extinguisher if your employees do not know how to use it properly in case of a fire? Here are three other examples of appropriate training:

- If you assign special security management tasks to an employee (as your information security officer, for instance), he or she will need wide-ranging knowledge of the methodological, organisational, and technical aspects of this field, along with constant opportunities to keep this knowledge up-to-date. The time this will require must be factored in before introducing such responsibilities and appointing an employee to bear them.
- If your organisation's interface with the Internet is to be protected by a firewall, the network administrator responsible will need to know how to install, configure, and oversee this component in a secure manner.
- Using encryption software to preserve the confidentiality of personal or business-critical data involves more than amassing knowledge of the software in question; rules also need to be set regarding how it should be used. What messages or files need to be encrypted? How should the private key be protected? How can you ensure that authorised representatives will be able to access encrypted data when necessary? You will need to make sure that your employees understand the answers you come up with to these and other questions.

Raise awareness among the employees affected!

Quality training alone is no guarantee of behaviour that supports security. To make sure that corresponding measures remain effective for the long term, it is important to raise employees' awareness of information security. They must also be willing to carry out such activities, observe the necessary directives, and (in some cases) accept provisions that may be inconvenient. Here are some negative examples:

- Fire doors are ineffective when they are held open by a door wedge because employees find it inconvenient to open them all the time.
- It makes little sense to invest in e-mail encryption software if your employees are going to continue sending unencrypted e-mails – even those with confidential content – because they are unaware of the related risks.
- Passwords always represent an additional step to be taken before the actual task at hand. Rules designed to ensure password security (through periodic changes or the use of different passwords for different systems, for instance) make them more inconvenient. If employees view these requirements as nothing but an annoying obligation, they will be more likely to circumvent them, such as by choosing insecure passwords or writing their passwords down and leaving them near their computers.
- If a network administrator discusses problems that have arisen in installing a security gateway and provides his or her work location in an online forum, the effectiveness of the protection provided by the software to be installed is at risk.

Whether in separate meetings, regularly occurring discussions, or in some written format, the purpose of new security measures must be explained to the employees affected in an understandable manner.

Check how well measures are being accepted!

Security measures that employees do not accept are likely to fail. Once you have implemented such measures, you should thus check whether your employees are actually following them. If they are not (or doing so only to a limited extent), you should attempt to identify the reasons why and initiate additional measures to raise awareness as required.

Unit 7.5: Documenting Plans

The following excerpt from RECPLAST's implementation plan demonstrates how you can document the decisions you have taken to put security measures in place. It lists measures pertaining to a select target object, print server S008, and decisions that have been taken regarding related deadlines, budget resources, and responsibilities.

Requirement	Measure planned	Planned deadline	Budget	Person responsible
SYS.1.1.A3 *Restrictive Granting of Access Rights*	The remaining group authorisations must be removed	Q3 of this year	No costs	Mr Schmitt (IT operations)
SYS.1.1.A4 *Separation of Roles*	Set up separate user IDs for each administrator	31 July	No costs	Mr Schmitt (IT operations)
SYS.1.1.A8 *Regular Data Backups*	Data backups are currently preserved on tapes in the server room. An external backup system is being planned, and a quotation for its initialisation has already been obtained (€15,000.00). The costs of running it still need to be negotiated.	Q1 of next year	Purchase: €15,000.00 Ongoing operations: TBD	Ms Meyer (Purchasing)

Table 19: Example of how to document implementation planning

Unit 7.6: Test questions

You have now completed the lesson on implementation planning. If you wish, you can use the following questions to test your knowledge of implementation planning in accordance with IT-Grundschutz. Please note that multiple answers may be correct.

1 **What do you need to check when planning the implementation of security measures?**

a What support measures are necessary to ensure a successful implementation

b Whether each measure is already in place

c Whether each measure is compatible with the others in question

d The order in which the different measures should be implemented

2 **What information from the IT-Grundschutz Compendium can help you plan the implementation of your measures in an order that makes sense?**

a The five code digits used to indicate the priority of requirements in the IT-Grundschutz modules

b The manner in which requirements are classified as basic, standard, or pertaining to higher protection needs

c The suggested approach to planning the implementation of modules in a sensible order based on the indicators R1, R2, and R3

d The threat situation presented at the beginning of each module

3 **As an information security officer, what should you do if your organisation's executives are not willing to provide the resources required to implement a given security measure?**

a You should point out the risks associated with a failure to implement the measure.

b You should ask the executives to sign a document confirming that they acknowledge and accept the threats at hand.

c You should ignore the executives and implement the measure anyway.

d You should forgo responding immediately, but plan to obtain the executives’ consent after a certain amount of time has passed.

4 **As a rule, who should implement technical measures designed to secure a given IT system?**

a The head of the IT department

b The information security officer

c The system administrator responsible

d Those who use the IT system

5 **In most cases, who should check whether a given security measure has been implemented as planned?**

a The organisation's executives

b The information security officer

c The IT administrator responsible

d The head of the IT department

6 **What resources in the IT-Grundschutz Compendium can you use to point out the risks associated with a failure to meet requirements to your organisation's executives?**

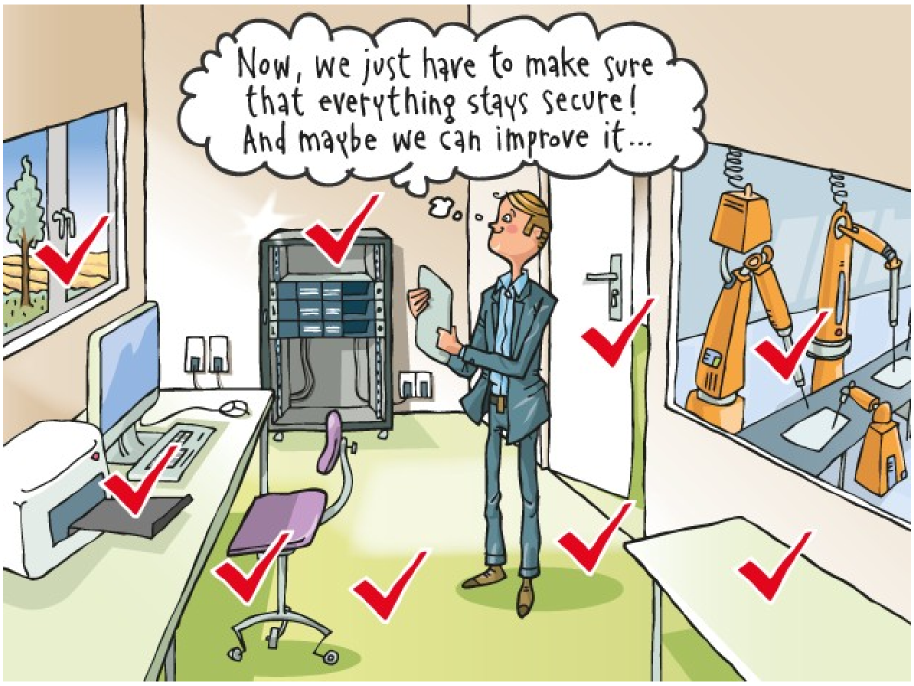
a The residual risk declaration form in the compendium's appendix

b The cross-reference table at the end of each module

c The risk calculation scheme found in the overview of elementary threats

d The examples of successful methods found in the module ORP.3 *Awareness-raising and training*

Lesson 8: Maintenance and improvement


Now, we just have to make sure that everything stays secure! And maybe we can improve it...

In your implementation plan, you have defined the measures you want to establish as part of your security concept, along with when and how you will do so. You have taken the necessary resources, support measures, and interim deadlines into account. To be sure that everything has been implemented and is working as planned, you will need to monitor your organisation's **compliance with these plans** on a regular basis.

Again, information security is not a status that remains constant once you achieve it; it is an **ongoing process** you will have to adjust to new and evolving challenges.

In this lesson, you will learn about methods you can use to **continuously monitor and improve the suitability and effectiveness** of your institution's technical and organisational measures to safeguard information security. You will learn about:

- How you can check the **implementation status** of the measures set forth in your security concept
- How you should proceed in reviewing the **effectiveness** of these measures
- How you can translate the results of your monitoring into **measures that will improve** your information security management
- How **key figures** can help you assess specific aspects of information security
- What a **maturity model** for information security involves and how it can be of use to you
- How you can provide third parties with evidence of the solid level of security you have achieved in the form of **ISO 27001 certification based on IT-Grundschutz**

Unit 8.1: Central questions for the monitoring efforts

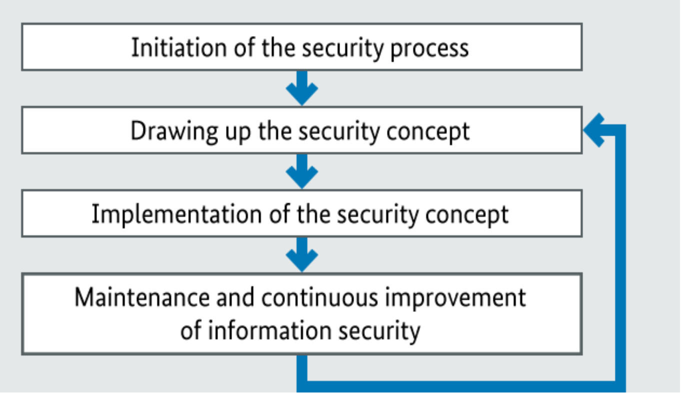

Initiation of the security process
Drawing up the security concept
Implementation of the security concept
Maintenance and continuous improvement of information security

Illustration 16: Phases of the security process

The measures in your security concept require continuous monitoring to ensure that they always meet the requirements at hand.

Monitoring efforts like these should be aligned with the following central questions:

- **What are the most pressing aims regarding information security at the moment?**

  The significance of individual security goals can evolve over time. For example, preserving the confidentiality of information can become more important if the surrounding legal conditions change or your organisation begins working with data that have stricter requirements in this regard. All measures designed to preserve confidentiality must thus be subject to particularly thorough monitoring. Another important question pertains to whether the security measures chosen still correspond to the threats at hand. You should also check whether new technical methods might offer more efficient and effective protection.

- **Who is responsible for monitoring the information security process?**

  Organisations are often so complex that an ISO cannot oversee and carry out all the necessary monitoring efforts on his or her own. This is when it is important to appoint multiple individuals to design and implement measures in different areas, document the results, and plan and manage corresponding improvements. When responsibilities are delegated in this manner, maintaining a good level of collaboration and informing the ISO of all the steps taken is key.

- **How often should methods be reviewed?**

  For protection mechanisms that are less important, checks do not need to be carried out as frequently as for critical processes. Your overall security concept should be reviewed at least once per year to determine whether it is still an effective means of fulfilling the information security objectives of your company or government agency. If a security incident occurs, this should serve as an opportunity to conduct an additional review.

The implementation recommendations in ISMS.1.M11: *Information security continuity* offer important advice on how to proceed in reviewing your security process.

Unit 8.2: Monitoring Methods

There are a number of proven approaches you can follow to monitor the efficiency and effectiveness of your information security measures. They range from completing simple checklists and conducting penetration tests in specific areas of network security to carrying out comprehensive reviews of how effective and appropriate the technical and organisational measures in place actually are.

As a general rule, comprehensive checks like these should be performed at **regular intervals** (either annually or with up to three years in between). That said, **reviews can also be helpful when the circumstances warrant them** – following changes in business processes, for example, and especially when a security incident has occurred.

Security incidents should always be taken as an opportunity to scrutinise your security concept. This should be done in an open and thorough manner to identify and eliminate vulnerabilities that gave rise to the incident at hand.

Information security audits and cyber security checks are two useful methods you can use to review your security concept and the level of protection you have achieved.

- In an **information security (IS) audit**, you can have professional auditors follow a defined approach to determine whether your organisation's security concept has been implemented as intended and still meets the latest requirements. An IS audit provides reliable information on the current status of information security to both the executives and those responsible for information security at your organisation. Along with a comprehensive audit that emphasises all the aspects and details of information security at your organisation, there are also compact, cross-sectional, and partial variants that limit the scope and depth of the audit to be conducted.
- If you do not yet have much experience in this area, a **cyber security check** can offer key assistance as you review the level of security at your organisation. It will provide indications of how susceptible your organisation is to cyber attacks and is designed to reduce the risk of falling victim to such attacks when conducted on a regular basis.

The separate procedural model the BSI has developed for carrying out IS audits is described in the Guide to IS Audits. There, you can also learn more about the scope and depth of these audits and the purposes behind the different variants of the procedure.
For information on carrying out cyber security checks and subsequent reporting, please refer to the corresponding action guideline. It also covers how this review procedure relates to IT-Grundschutz and other key standards of information security.

Managing the results of reviews

The **results** of all types of reviews must be **documented** and **presented to your organisation's executives**. In particular, they need information on the status of implemented measures, the accomplishments and problems thus far, and risks stemming from implementation deficiencies. If certain aspects have not gone to plan, suggestions on how they should be adjusted or the implementation should be corrected must be formulated. The same applies to suggestions regarding the improvement and ongoing development of the security measures implemented. All decisions taken on these subjects, as well as the acknowledgement of risks arising from the delayed implementation of measures, must be documented.

Standard requirements that reports to the executive level SHOULD fulfil are described in module ISMS.1 *Security Management* of the IT Grundschutz Compendium under ISMS.1.A12 *Management Reports on Information Security*.

Unit 8.3: Key Figures

Key figures can serve as indicators of the quality of the entire security process or that of its individual sub-processes and aspects. They are a proven instrument that can be used to communicate both achievements and problems in information security to the executives of a given organisation.

The following table contains examples of potential key figures for various layers of the IT-Grundschutz Compendium. These examples show that key figures can document both technical and organisational aspects of information security.

Module	Requirement	Key figure
ISMS.1 *Security Management*	The executive level SHOULD be informed of the status of information security on a regular basis.	Number of executive meetings featuring a security report / number of all executive meetings
ORP.2 *Personnel*	The tasks and responsibilities of employees SHOULD be documented in a suitable manner.	Number of employee contracts that specify an obligation to handle information in a secure manner / number of all employee contracts
CON.3 *Data backup policy*	Data backups and any restoration procedure that may be required SHOULD be tested on a regular basis.	Number of successful tests / total number of tests of data backup restoration
OPS.1.1.2 *Proper IT administration*	The authorisations, tasks, and obligations of IT administrators SHOULD be defined in a binding manner in work instructions or guidelines.	Number of work instructions / number of all administrators
DER.1 *Detection of security-relevant events*	The event notifications collected from IT systems and application systems SHOULD be stored in a centralised logging infrastructure.	Number of event notifications collected centrally / number of all event notifications
APP.1.1 *Office products*	New Microsoft Office products SHOULD be tested for compatibility with established work resources before being put into use.	Number of tested Microsoft Office products in use / Number of all Microsoft Office products in use
SYS.1.1 *General server*	The procedure, framework conditions, requirements for administrative tasks, and separation of duties among the different roles of the IT system users in question SHOULD be defined in a user and administration concept.	Number of servers with a detailed administration concept / number of all servers

Tabele 20: Examples of key figures on information security

These examples show that a large number of key figures are necessary to render a comprehensive assessment of information security. In some cases, collecting, calculating, and refining key figures requires a great deal of resources; that said, technical key figures can often be produced automatically, which typically results in lower resource requirements than those pertaining to organisational key figures.

To ensure that the resources required are proportionate to the results produced, it is important to formulate the objectives of key figures clearly and accurately estimate the effort that will be necessary to collect the corresponding measurements. If you are planning to introduce key figures on information security at your organisation, it is a good idea to start with a small number of figures and add to them gradually as you gain further experience.

Unit 8.4: Maturity Models

To obtain an all-encompassing overview of the quality of your information security process, you can use a maturity model. This involves analysing and evaluating your organisation's ISMS over a period of years. The maturity of the overall ISMS (or parts thereof) is determined based on the **degree to which the process is structured and systematically controlled**.

The following table offers an example of how **levels of maturity can be defined**:

Maturity level	Identifier
0	No process exists, nor are there plans to create one.
1	There are plans to establish a process, but nothing has been implemented.
2	Parts of the process have been implemented, but no systematic documentation has been produced.
3	The process has been fully implemented and documented.
4	The effectiveness of the process is also reviewed on a regular basis.
5	In addition, measures are in place to ensure continuous improvement.

Table 21: Example of how to define maturity levels

In applying a maturity model, the aim is to improve quality in all the individual areas of your ISMS. Through regular analyses, you can identify processes that are not yet subject to sufficient controls.

The following graphic presents an example of the maturity levels reached in various topic areas at an organisation. Action is particularly urgent in areas that exhibit a low maturity level. Maturity models can thus help you determine what you should focus on in the ongoing development of your ISMS.

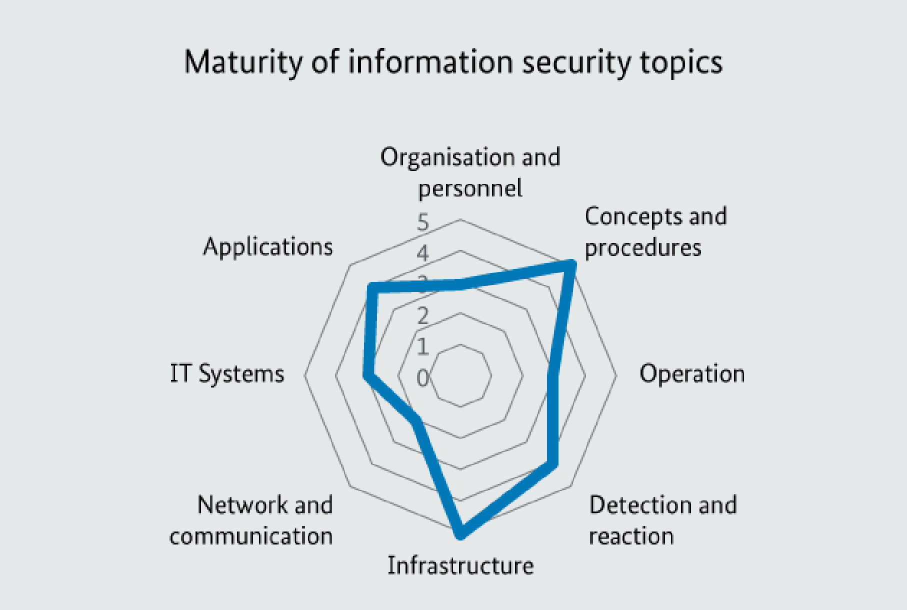


Illustration 17: Example of maturity level visualisation

Unit 8.5: IT-Grundschutz Certification

Generally recognised certification sets **standards** and engenders **trust**. Information security is another area in which reliable standards are beneficial, as they help users understand how secure products, systems, and procedures are. This is why internationally recognised sets of criteria have existed for years to serve as a basis on which independent certification bodies can confirm the security characteristics of such products and systems.

ISO 27001 certification based on IT-Grundschutz provides special affirmation of an organisation's information security efforts, as obtaining it requires not only the fulfilment of the general security management requirements of the ISO 27001 norm, but documented implementation of the much more specific requirements set forth by IT-Grundschutz, as well.

Information security management certification can be of interest to **various target groups**, including:

- Providers involved in e-commerce or e-government that want to emphasise how careful they are in keeping the data of customers and citizens secure
- IT service providers that want to provide evidence of how secure their services are based on a generally recognised standard
- Companies and government agencies that want to cooperate with other institutions and need information on their security levels

Certification procedures can also have an **internal effect** by making employees more aware of the necessity of information security, which in turn facilitates the process of implementing the security measures required.

The certification process

One prerequisite of obtaining ISO 27001 certification based on IT-Grundschutz is proof that **information security management** corresponding to the requirements of the norm has been established and that the **IT-Grundschutz requirements** have also been effectively met. The object of certification need not be the entire organisation at hand. The information network under review can also be limited to individual business processes, specialised tasks, or organisational units. These elements must, however, be delineated in a sensible manner and have a certain minimum scope.

The following figure illustrates the **certification process**:

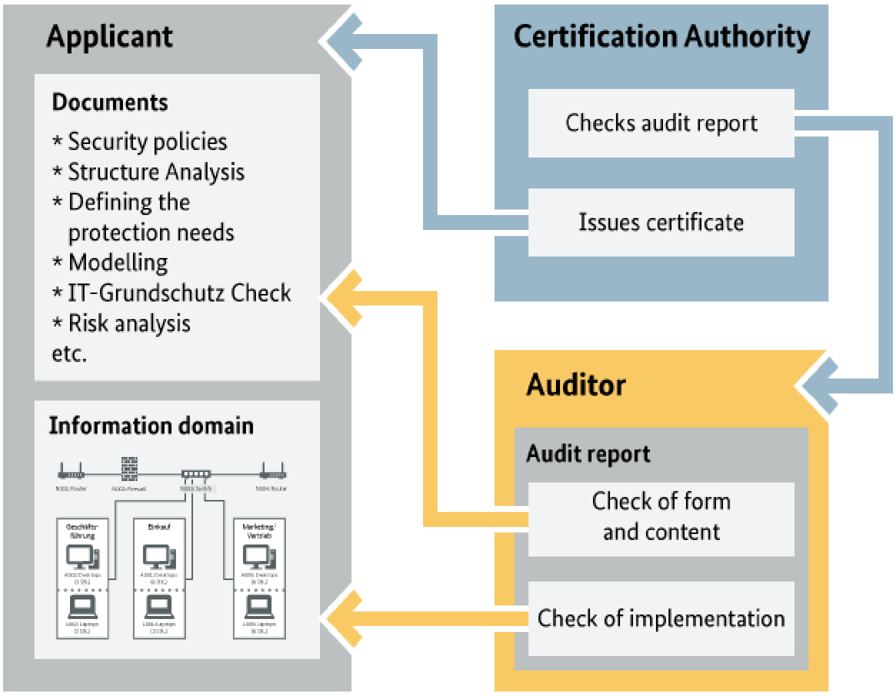


Illustration 18: The process of obtaining ISO 27001 certification based on IT-Grundschutz

To confirm that the relevant requirements have been met, an audit must be conducted by an independent auditor recognised by the BSI. In principle, each audit consists of two separate phases that build on one another:

- **Phase 1** involves a **review of the reference documents** provided by the applicant. Along with the applicable security guidelines (for information security, risk analysis, and internal ISMS auditing) and the applicant's plan for dealing with risks, this particularly includes the documented results of the various phases of designing a security concept (structural analysis, determining protection requirements, modelling, the IT-Grundschutz check, risk analysis, and implementation planning).
- In **phase 2**, the auditor **reviews the implementation** of the measures described in the reference documents with a focus on completeness, correctness, effectiveness, and how well the measures conform to the requirements of ISO 27001 and IT-Grundschutz.

Certification is only granted when the resulting audit report renders a positive overall verdict and is accepted by the certification body in question. As part of evaluation monitoring, the audit report is also checked against the specifications of the certification scheme published by the BSI.

Certification remains **valid for three years** and must be confirmed by **annual monitoring audits**.

The certification scheme at the heart of ISO 27001 certification based on IT-Grundschutz, notes on the reference documents required, and all other important information on this subject have been combined into a separate sub-topic on the BSI website.

Unit 8.6: Test questions

You have reached the end of the lesson. If you wish, you can use the following questions to test your knowledge of how information security can be maintained and improved. Please note that multiple answers may be correct.

1 **Why should you review your security concept on a regular basis?**

a Because threats evolve

b Because your organisation's processes and structures evolve

c Because your organisation's objectives and priorities evolve

d Because the IT security industry is constantly influenced by new trends

2 **What criteria should you take into account when reviewing your security concept?**

a How up-to-date the security concept is

b The security concept's scope

c Whether the security concept will be accepted by your organisation's executives

d How complete the security concept is

3 **What advantages do maturity models offer in assessing an ISMS?**

a A maturity model can be used to evaluate how structured a process is and the extent to which it is subject to systematic controls.

b Applying a maturity model is a prerequisite of obtaining IT-Grundschutz certification.

c A maturity model can be applied to specific aspects of an ISMS to reveal deficiencies in individual processes.

d Applying a maturity model fulfils a central requirement of the ISO 27001 norm.

4 **What prerequisites must be met to obtain ISO 27001 certification based on IT-Grundschutz?**

a Only the basic requirements must be fulfilled and confirmed by an audit.

b After viewing corresponding documents and conducting on-site inspections, a certified auditor must confirm that the IT-Grundschutz requirements have been met.

c The BSI must render a positive assessment upon reviewing the corresponding audit report.

d The organisation in question must submit a declaration confirming that it has fulfilled all of the IT-Grundschutz requirements and have it signed by a certified auditor.

5 **Which of the following examinations are meant to serve as part of a systematic review of information security at a given organisation?**

a Analyses of IT security incidents

b penetration tests

c IT security audits

d Audits conducted as part of ISO 27001 certification based on IT-Grundschutz

6 **What should always be established before a key figure related to information security is introduced?**

a The intended purpose of the key figure

b The stylistic devices to be used in marking results as positive or negative

c The procedure to be followed in collecting values associated with the key figure

d A way to conceal the results from the organisation's executives

Outlook

You have now completed the online course on IT-Grundschutz. We hope you have gained solid insights into the IT-Grundschutz methodology and how you can make use of the IT-Grundschutz Compendium.

Further information and resources pertaining to IT-Grundschutz are available on the adjacent webpages. If you have any related questions or comments, please feel free to contact us by phone or e-mail.

Appendix: solutions to test questions

Accurate statements are labelled as [**correct**].

On Lesson 1: Security Management

1 **Which model is based on the security process described in BSI Standard 200-1?**

a A cycle comprising four steps: plan, do, check, and act [**correct**]

b a method to define the state-of-the-art information security level

c A model designed to facilitate continuous improvement [**correct**]

d a model of technical security safeguards

2 **Was should an information security policy contain?**

a detailed technical requirements for configuring important IT systems

b Statements on the importance of information security for the organisation in question [**correct**]

c Fundamental rules on organising information security [**correct**]

d specific behavioural rules on handling confidential information

3 **For which tasks is an information security officer typically responsible?**

a Coordinating the development of security concepts [**correct**]

b configure the security technology used

c Reporting to the executive level on the current information security status [**correct**]

d answer questions from the media related to the status of information security in companies

4 **What is an appropriate way to build an IS management team?**

a Each department of a company or government agency sends employees, ensuring that all areas are covered.

b The IT manager alone appoints several employees to the team.

c The composition is on a volunteer basis. Anyone who is interested will be included.

d Management assembles the team from those responsible for certain IT systems, applications, data protection, IT service and (if available) ICS-ISB. [**correct**]

5 **Who is responsible for approving the information security policy?**

a The IS management team

b ISB

c The executives at the company or government agency at hand [**correct**]

d PR department in a company or government agency

6 **Why could it be useful to decide on a security concept in accordance with Basic Protection?**

a Meeting the associated requirements is entirely sufficient for a normal company in most cases.

b The organisation in question needs to achieve information security in short order and the Basic Protection presents a suitable entry point. [**correct**]

c The organisation in question wants to achieve information security incrementally. In the medium term, the security concept in accordance with standard security can be expanded. [**correct**]

d There is an urgent need to protect valuable information The Basis Protection provides for suitable protection of an organisation's “crown jewels”

On Lesson 2: Structural Analysis

1 **What are objectives of structural analysis within the context of IT-Grundschutz Methodology?**

a Identifying objects that are exposed to particularly significant risks

b Identifying objects that a corresponding security concept needs to cover [**correct**]

c Assembling objects to which the same security measures can be applied into suitable groups [**correct**]

d Determining the objects for which there are appropriate modules in the IT-Grundschutz Compendium

2 **What information can be found in networks that are necessary for a structural analysis?**

a The organisational units involved in drafting the security concept

b The type of connections linking the IT systems in the information network at hand [**correct**]

c The external network connections of the information network at hand [**correct**]

d The type of IT systems in the information network at hand [**correct**]

3 **When would it be useful to group IT systems during a structural analysis?**

a When they have the same protection requirements and similar characteristics (operating system, network connection, supported applications) [**correct**]

b When these systems have their own appropriate modules in the IT-Grundschutz Compendium

c When they share the same premises

d When the total number of objects documented is growing too large

4 **Which of the following tasks are part of structural analysis according to BSI Standard 200-2?**

a Grouping together the components of an information network in a suitable manner [**correct**]

b Modelling the business processes and specialised tasks within an information network

c Checking whether the IT in use provides adequate support to the business processes and specialised tasks at hand

d Documenting the information, business processes, applications, IT systems, communication connections, and spatial conditions in the information network at hand [**correct**]

5 **What information on IT systems must be documented during a structural analysis?**

a Type and purpose of use [**correct**]

b Supplier and price

c The system's users and administrator [**correct**]

d Location (building and room) [**correct**]

6 **What applications must be documented during structural analysis?**

a All the applications installed on the IT systems of the information network at hand

b All applications that are required by at least one of the business processes documented [**correct**]

c All applications for which a valid licence is available

d All applications that are used by at least 20% of an organisation's employees

On Lesson 3: Determining Protection Requirements

1 **What traditional objectives are recommended when determining protection requirements in accordance with IT-Grundschutz?**

a Authenticity

b Availability [**correct**]

c Confidentiality [**correct**]

d Integrity [**correct**]

2 **In what cases can you forgo determining an IT system's protection requirements in accordance with IT-Grundschutz?**

a When the IT system is to be decommissioned within 18 months

b When the IT system is not used [**correct**]

c When the applications it supports only have normal protection requirements

d When the protection requirements in question were already determined in an audit conducted one year before

3 **What criteria do you need to take into account when determining an IT system's availability requirements?**

a The maximum system downtime that can be tolerated [**correct**]

b The effort required to restore the IT system following a breakdown

c The number of people who use the IT system

d The costs of procuring the IT system

4 **What do you need to consider when determining the protection requirements of an application?**

a The information used in connection with the application [**correct**] b The application's significance with regard to business processes or specialised tasks [**correct**]

c The relevant risks to which the application is exposed

d The physical environment of the IT system that makes the application available

5 **Under what circumstances can the protection requirements regarding an IT system's availability be lower than those of the applications for which it is used?**

a When the accounting value of the IT system falls below a previously defined threshold

b When the IT system only serves components of the respective applications that have lower protection requirements [**correct**]

c When at least one other redundant IT system is in use that can make the applications available [**correct**]

d When the applications are to be restructured in a manner that will no longer require the IT system within the next three months

6 **When cumulative effects are to be taken into account in determining an IT system's protection requirements, this means that...**

a ...the IT system has higher protection requirements because individual instances of damage could add up to a greater amount of overall damage [**correct**]

b ...the IT system has lower protection requirements because appropriate and mutually complementary safeguards are in place

c ...the protection requirements determined for the IT system also affect the requirements of other IT systems that are connected to the system in question

d ...the IT system's protection requirements cannot be determined until the requirements of the IT systems connected to it are determined

On Lesson 4: Modelling

1 **What tasks do you need to perform during modelling in accordance with IT-Grundschutz?**

a You must use the IT-Grundschutz modules to map the information network identified during structural analysis. [**correct**]

b You must draw up a security architecture for the information network under review.

c You must mark target objects that cannot be adequately modelled for subsequent risk analysis. [**correct**]

d You must check whether IT-Grundschutz modules are relevant to the information network under review. [**correct**]

2 **What information does an IT-Grundschutz module contain?**

a Details on specific threats [**correct**]

b Descriptions of standard security measures

c References to further information [**correct**]

d Security requirements pertaining to a given situation [**correct**]

3 **What tasks do you need to perform after determining which modules will be applied to your information network and its individual target objects during modelling?**

a You must define measures through which the requirements at hand can be met. [**correct**]

b You must check whether alternatives are necessary for individual requirements that cannot be met with a reasonable amount of resources in the application context at hand. [**correct**]

c You must adjust the protection requirements determined for target objects for which the fulfilment of said requirements seems unrealistic.

d You must document the results of the modelling process. [**correct**]

4 **What should you bear in mind when selecting and adjusting security measures based on the respective requirements?**

a How cost-efficient the measures are [**correct**]

b How effective the measures are [**correct**]

c How innovative the measures are

d How user-friendly the measures are [**correct**]

5 **Which statements regarding the application of modules to servers apply?**

a The module SYS.1.1 *General server* should only be applied when there is no operating-system-specific module for the server in question.

b Along with module SYS.1.1 *General server*, the relevant operating-system-specific module should always be applied. [**correct**]

c When special modules are available for server applications (web or database servers, for example), the relevant operating-system-specific module does not need to be applied.

d For virtualisation servers, the module SYS.1.1 *General server* and the relevant operating-system-specific module must both be applied along with the module for virtualisation servers. [**correct**]

6 **To what target objects does the module ISMS.1** *Security management* **need to be applied during modelling?**

a It MUST be applied separately to each location of a significant size within the information network at hand.

b It MUST be applied once to the entire information network. [**correct**]

c It is only relevant if the information network is of a certain minimum size.

d It MUST be applied separately to every sub-network identified during structural analysis.

On Lesson 5: IT-Grundschutz Checks

1 **Which statements regarding IT-Grundschutz checks are correct?**

a An IT-Grundschutz check makes it possible to identify areas in which security requirements have not been met. [**correct**]

b An IT-Grundschutz check only covers the fulfilment of basic requirements.

c An IT-Grundschutz check serves to identify security problems that must then be examined in greater detail in a risk analysis.

d An IT-Grundschutz check compares security requirements against the security measures that have actually been implemented. [**correct**]

2 **What preparations does an IT-Grundschutz check require?**

a A schedule must be set. [**correct**]

b Appropriate interview partners must be selected. [**correct**]

c A penetration test must be carried out to identify vulnerabilities that will be discussed with the interview partners chosen.

d Available documents on information security in the information network under review must be collected and read. [**correct**]

3 **What procedures should you follow to determine how well a group of clients is protected during an IT-Grundschutz check?**

a You should conduct interviews with the system administrators responsible. [**correct**]

b In a penetration test, you should attempt to identify vulnerabilities in the IT systems in question while incorporating all the clients belonging to the group.

c You should perform on-site examinations of random clients and their configurations. [**correct**]

d You should read available documentation on the clients' configurations. [**correct**]

4 **When should you assess a requirement of a given IT-Grundschutz module as fulfilled during an IT-Grundschutz check?**

a When the requirement is fully covered by appropriate and effective measures [**correct**]

b When the corresponding interview partner has given you credible assurances that there have not been any security issues with the IT system in question thus far

c When there is extensive documentation on the protective measures that have been implemented for the IT system in question

d When neither random checking nor the interview conducted with the person responsible for the IT system has revealed any security flaws [**correct**]

5 **How should you proceed in dealing with specifications for higher protection requirements during a first-time IT-Grundschutz check (that is, before carrying out risk analyses)?**

a As a rule, you should classify these specifications as unnecessary and also forgo checking them once they have been implemented at your organisation.

b You should remove these specifications from your target concept.

c You should examine the specifications for high and very high protection requirements only after your risk analysis is complete. [**correct**]

d As a rule, you should examine all the specifications cited in the IT-Grundschutz modules during an IT-Grundschutz check, including those pertaining to higher protection requirements.

6 **You discover that a standard requirement has not been met for an IT system that will soon be decommissioned. How should you treat this requirement in an IT-Grundschutz check?**

a You should remove the requirement from your IT-Grundschutz model.

b You should document the requirement as unnecessary, as fulfilling it would no longer be cost-efficient.

c You should document the requirement as not fulfilled and consider including a note that measures meant to address this shortcoming should be reviewed in terms of their cost-efficiency due to the impending decommissioning of the IT system in question. [**correct**]

d You should document the requirement as not fulfilled and include a note that the resulting risks should be reviewed in terms of whether they are acceptable due to the impending decommissioning of the IT system in question. [**correct**]

On Lesson 6: Risk Analysis

1 **Who bears responsibility for the decisions taken regarding a given IT system during risk analysis?**

a The IT system's administrator

b The organisation's executives [**correct**]

c The information security officer

d The IS management team

2 **Which threats are examined in the first step of creating a threat overview?**

a The risk catalogues found in the appendix to BSI Standard 200-3

b The relevant elementary threats from the IT-Grundschutz Compendium [**correct**]

c The threats listed in the appendix to the ISO 27005 norm

d The specific threats listed in a module's sections on the threat situation at hand

3 **What should you evaluate when assessing risk?**

a How frequently a threat occurs [**correct**]

b The scale of damage associated with a threat [**correct**]

c The protection objectives impacted by a threat

d The effectiveness of the measures planned and already implemented to address a threat

4 **How can you transfer risk?**

a By taking out an insurance policy [**correct**]

b By outsourcing a high-risk business process to an external service provider [**correct**]

c By restructuring a high-risk business process

d By deciding to take risk-mitigating measures only after the necessary financial resources become available

5 **What reasons may justify accepting a high level of risk?**

a Potential safeguards would require an inordinate amount of resources. [**correct**]

b Similar organisations also accept the risk in question.

c There are no effective safeguards against the risk in question. [**correct**]

d The threat from which the risk stems has not led to a significant security incident thus far.

6 **In principle, when can a risk not be accepted?**

a When basic requirements are not fulfilled [**correct**]

b When elementary threats are present

c When a situation calls for very high protection requirements

d When standard requirements are not fulfilled

On Lesson 7: Implementation Planning

1 **What do you need to check when planning the implementation of security measures?**

a What support measures are necessary to ensure a successful implementation [**correct**]

b Whether each measure is already in place

c Whether each measure is compatible with the others at hand [**correct**]

d The order in which the different measures should be implemented [**correct**]

2 **What information from the IT-Grundschutz Compendium can help you plan the implementation of your measures in an order that makes sense?**

a The five code digits used to indicate the priority of requirements in the IT-Grundschutz modules

b The manner in which requirements are classified as basic, standard, or pertaining to higher protection needs [**correct**]

c The suggested approach to planning the implementation of modules in a sensible order based on the indicators R1, R2, and R3 [**correct**]

d The threat situation presented at the beginning of each module

3 **As an information security officer, what should you do if your organisation's executives are not willing to provide the resources required to implement a given security measure?**

a You should point out the risks associated with a failure to implement the measure. [**correct**]

b You should ask the executives to sign a document confirming that they acknowledge and accept the threats at hand. [**correct**]

c You should ignore the executives and implement the measure anyway.

d You should forgo responding immediately, but plan to obtain the executives’ consent after a certain amount of time has passed.

4 **As a rule, who should implement technical measures designed to secure a given IT system?**

a The head of the IT department

b The information security officer

c The system administrator responsible [**correct**]

d Those who use the IT system

5 **In most cases, who should check whether a given security measure has been implemented as planned?**

a The organisation's executives

b The information security officer [**correct**]

c The IT administrator responsible

d The head of the IT department

6 **What resources in the IT-Grundschutz Compendium can you use to point out the risks associated with a failure to meet requirements to your organisation's executives?**

a The residual risk declaration form in the compendium's appendix

b The cross-reference table at the end of each module [**correct**]

c The risk calculation scheme found in the overview of elementary threats

d The examples of successful methods found in the module ORP.3 *Awareness-raising and training*

On Lesson 8: Maintenance and Improvement

1 **Why should you review your security concept on a regular basis?**

a Because threats evolve [**correct**]

b Because your organisation's processes and structures evolve [**correct**]

c Because your organisation's objectives and priorities evolve [**correct**]

d Because the IT security industry is constantly influenced by new trends

2 **What criteria should you take into account when reviewing your security concept?**

a How up-to-date the security concept is [**correct**]

b The security concept's scope

c Whether the security concept will be accepted by your organisation's executives

d How complete the security concept is [**correct**]

3 **What advantages do maturity models offer in assessing an ISMS?**

a A maturity model can be used to evaluate how structured a process is and the extent to which it is subject to systematic controls. [**correct**]

b Applying a maturity model is a prerequisite of obtaining IT-Grundschutz certification.

c A maturity model can be applied to specific aspects of an ISMS to reveal deficiencies in individual processes. [**correct**]

d Applying a maturity model fulfils a central requirement of the ISO 27001 norm.

4 **What prerequisites must be met to obtain ISO 27001 certification based on IT-Grundschutz?**

a Only the basic requirements must be fulfilled and confirmed by an audit.

b After viewing corresponding documents and conducting on-site inspections, a certified auditor must confirm that the IT-Grundschutz requirements have been met. [**correct**]

c The BSI must render a positive assessment upon reviewing the corresponding audit report. [**correct**]

d The organisation in question must submit a declaration confirming that it has fulfilled all of the IT-Grundschutz requirements and have it signed by a certified auditor.

5 **Which of the following examinations are meant to serve as part of a systematic review of information security at a given organisation?**

a Analyses of IT security incidents

b penetration tests

c IT security audits [**correct**]

d Audits conducted as part of ISO 27001 certification based on IT-Grundschutz [**correct**]

6 **What should always be established before a key figure related to information security is introduced?**

a The intended purpose of the key figure [**correct**]

b The stylistic devices to be used in marking results as positive or negative

c The procedure to be followed in collecting values associated with the key figure [**correct**]

d A way to conceal the results from the organisation's executives