Bundesamt
für Sicherheit in der
Informationstechnik

Instructions on security concept migration

Resources to achieve modernised IT-Grundschutz

Change history

Version	Date	Author	Description
1.0	01/03/2018	BSI	1st published version

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

Table of contents

Change history 2
1 Introduction 5
1.1 Target group 5
1.2 Notes on application 5
1.3 Structure of migration instructions 6
2 Overview of BSI standards 7
2.1 Previous IT-Grundschutz 7
2.2 Modernised IT-Grundschutz 7
2.3 Significant changes 8
3 Instructions on migration 10
3.1 Structure analysis 10
3.2 Determining protection requirements 11
3.3 Modelling 11
3.4 IT-Grundschutz check 13
3.5 Risk analysis 14
4 Resources 17
4.1 Implementation notes 17
4.2 Tools 17
4.3 Migration tables 17
References 21

1 Introduction

Since being introduced in 1994, the BSI's IT-Grundschutz has been developed constantly further and is a reference work for information security in Germany. IT-Grundschutz underwent major revisions in 2005 to adjust to user requirements and, in particular, to international developments. Among other things, the previous IT-Grundschutz manual was split into the BSI standards 100-1, 100-2 and 100-3 and the IT-Grundschutz Catalogues. New chapters and recommendations have been added regularly to the IT-Grundschutz Catalogues, allowing the documentation to keep up with the diverse and rapid changes in information technology.

IT-Grundschutz was revised at a basic level again in 2017. In the course of modernising IT-Grundschutz, the existing IT-Grundschutz methodology, now called basic safeguards, has been extended to include two additional methodologies: basic safeguards and core safeguards. In addition, the BSI standards 100-1, 100-2 and 100-3 have been replaced by the BSI standards 200-1, 200-2 and 200-3. Not only that, but the IT-Grundschutz modules are now leaner, after having been restructured. The IT-Grundschutz Catalogues have thus been replaced by the IT-Grundschutz Compendium. For more information and all current publications, see [GSM].

The migration to modernised IT-Grundschutz in accordance with BSI standards 200-1, 200-2 and 200-3 affects any information security management system (ISMS) that was built with the previous IT-Grundschutz Methodology in accordance with BSI standards 100-1, 100-2 and 100-3, and the IT-Grundschutz Catalogues. These instructions on migration allow the BSI to support users of IT-Grundschutz whilst migrating from classic to modernised IT-Grundschutz and allows a smooth transition.

1.1 Target group

These instructions are intended exclusively for entities who already operate an ISMS in compliance with IT-Grundschutz in accordance with the BSI standards 100-1, 100-2 and 100-3 and which now intend to migrate to the modernised IT-Grundschutz in accordance with the BSI standards 200-1, 200-2 and 200-3 . Institutions that wish to start building an ISMS in accordance with IT-Grundschutz are recommended to start with BSI 200-2 directly.

1.2 Notes on application

This document describes how to migrate from a security concept based on BSI Standard 100-2 to the new BSI Standard 200-2. At the same time, it provides instructions on migrating from the IT-Grundschutz catalogues to the IT-Grundschutz Compendium.
This document is based on the assumption that the given entity has selected the standard safeguard methodology for its migration. Those entities that would like to restrict their scope and do not want to implement core safeguards for their existing ISMS may adapt these instructions accordingly. We do not recommend migrating from the IT-Grundschutz Methodology to 100-2 under the basic safeguards.

Similarly to the update to IT-Grundschutz, other contexts have changed, meaning that adaptation may require both modernised IT-Grundschutz and content changes to the security concept. These instructions on migration do not handle in detail how content may change during a migration of the security concept. It is possible that additional safeguards may be necessary to meet requirements.

The migration to modernised IT-Grundschutz also affects certified information systems that were audited and received certification based on the previous requirements.

In addition, grandfathering periods and options for migration within the context of certification are planned (see [FRIST].

1.3 Structure of migration instructions

Chapter 2 provides an initial overview of the BSI standards and of both the previous and modernised IT-Grundschutz.

Chapter 2 then takes a step-by-step approach to migrating an existing security concept to the modernised IT-Grundschutz. The presentation covers all phases of the IT-Grundschutz methodology, from structure analysis to determining protection requirements, modelling and the IT-Grundschutz check down to the risk analysis.

Chapter 4 is about resources and how they can be used to simplify the migration from classic to modernised IT-Grundschutz. The chapter also discusses the migration tables in detail.

2 Overview of BSI standards

Before we turn to the subject at hand, migrating security concepts, we first present the key principles and content of both the old and new standards in the following. In particularly, this will include a brief description of the key changes between IT-Grundschutz in accordance with BSI Standard 200-2 and IT-Grundschutz in accordance BSI Standard 100-2. In addition, the focus will be on activities relevant to creating a security concept in accordance with IT-Grundschutz, specifically structure analysis, defining the protection needs, modelling of an information system, IT-Grundschutz check and risk analysis.

2.1 Previous IT-Grundschutz

The previous IT-Grundschutz is described in the following documents:

- BSI Standard 100-1: Information Security Management Systems (ISMS) [BSI1001]
- BSI Standard 100-2: IT-Grundschutz Methodology [BSI1002]
- BSI Standard 100-3: Risk analysis based on IT-Grundschutz [BSI1003]
- IT-Grundschutz catalogues updated regularly via supplements

While the deprecated BSI Standard 100-1 primarily described the basic principles and the structure of an ISMS, the actual IT-Grundschutz method has now been shown in the deprecated BSI 100-2. It listed the following phases:

- Structure analysis
- Protection requirements determination
- Modelling
- Basic security check
- Supplementary security analysis
- Risk analysis

Requests for ISMS certification on the basis of BSI Standard 100-2 may be made until 30/09/2018 (see [FRIST]); the 15th supplement to the IT-Grundschutz catalogues will be able to be used until 30/09/2021 (see [PRUEF]).

2.2 Modernised IT-Grundschutz

IT-Grundschutz modernised in 2017 is described in the following documents:

- BSI Standard 200-1: Information Security Management Systems (ISMS)
- BSI Standard 200-2: IT-Grundschutz Methodology [BSI2002]
- BSI Standard 200-3: Risk analysis based on IT-Grundschutz [BSI2003]
- IT-Grundschutz Compendium (Edition 1, 2018) [GSKO]

The IT-Grundschutz Methodology described in BSI Standard 200-2 provides for three different methods:

- Basic safeguards
- Standard safeguards

- Core safeguards

These instructions on migration focus on entities which have already established an ISMS in compliance with IT-Grundschutz and have now selected the standard safeguards to update their security concept. For this reason, this document will discuss only the standard safeguards. They include the following phases:

- Structure analysis
- Protection requirements determination
- Modelling
- IT-Grundschutz check
- Risk analysis

2.3 Significant changes

The following significant changes were made in BSI Standard 200-2 in comparison with BSI Standard 100-2. For details, please see Chapter 3.

Structure analysis

As before, the scope must be defined exactly. However, the business processes within the scope are now the central starting point for the security concept. In a first step, the core business processes or specialised tasks included in the defined information system must be recorded and documented in this system. In this phase, based on every business process and/or every specialised task, the related applications and the information processed with them must be identified. In addition, the structure analysis must include the relevant service providers. Furthermore, IT systems are more starkly differentiated, requiring industrial controlling systems (ICS) and other devices (e.g. Internet of Things) to be included in the security concept. See Section 3.1 for detailed information on the structure analysis.

Determining protection requirements

The requirements for protection are defined based on the definition of protection requirements for the business processes (rather than for the applications, as was the case previously). This also applies to the remaining target objects of the scope (e.g. applications or IT systems). How protection requirements are determined shall be presented in Section 3.2 in detail.

Modelling

In the modelling phase, relevant modules of the IT-Grundschutz Compendium will continue to be identified. However, take note that the modules have been reworked completely and restructured. The modules are now organised in a new layer-based module as to whether they are process-orientated or system-orientated. The process-orientated modules are included in the following layers:

- ISMS: information security management systems
- ORP: organisation and personnel
- CON: concepts and methodologies
- OPS: operation
- DER: detection and reaction

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

- APP: applications

- SYS: IT systems
- IND: industrial IT
- NET: networks and communication
- INF: infrastructure

Not only have the names, structure and content of the modules changed, but also their basic alignment: while security safeguards were previously described in the modules, the modernised IT-Grundschutz merely formulates requirements. This permits freer selection of concrete safeguards at a given entity to fulfil a requirement. Naturally, this additional step of identifying appropriate safeguards for each requirement must be documented. Implementation notes are resources provided for many IT-Grundschutz modules. They describe how the requirements of the modules can be implemented and explain suitable security safeguards in detail. These implementation notes are merely sample best practices and are not binding. For detailed information on modelling, see Section 3.3.

IT-Grundschutz check

In the IT-Grundschutz check phase, a check is performed for each module and each requirement to determine whether a given requirement is fulfilled satisfactorily. Due to the above-mentioned paradigm shift, both the implementation of a concrete safeguard and the appropriateness of the safeguard for meeting the requirement must be checked. The IT-Grundschutz check is described in Section 3.4 in detail.

Risk analysis

The supplementary security analysis has been eliminated under the modernised IT-Grundschutz. Instead, a risk analysis is performed directly for target objects

- for which a higher degree of protection is required
- which cannot be adequately depicted (modelled) with the existing IT-Grundschutz modules
- which are used in operating scenarios (environment, application) that are not planned in the scope of IT-Grundschutz

BSI Standard 200-3 depicts a possible method of analysing and handling risks. This standard has undergone many changes in comparison to the predecessor standard 100-3. Some examples of changes follow: complete migration of the risk analysis to the elementary threats, the introduction of a matrix approach to assessing risks and the introduction of risk appetite and opportunity management. As before, additional security safeguards are included in the security concept. See Section 3.5 for more information on risk analysis.

An ISMS that has been established on the basis of BSI Standard 200-2 can audited and certified. Auditing and certification schemes are available for this purpose (see [AUD] and [ZERT]).

3 Instructions on migration

The following is a step-by-step description of how one can migrate existing security concepts based on the BSI standards 100-1, 100-2 and 100-3 and IT-Grundschutz Catalogues to the modernised IT-Grundschutz (in accordance with BSI standards 200-1, 200-2 and 200-3, and the IT-Grundschutz Compendium). This document assumes that an information security management system (ISMS) based on BSI Standard 100-2 and on the IT-Grundschutz Catalogues exists.

The first, essential step for an entity is to familiarise itself with the new BSI standards and the IT-Grundschutz Compendium. Familiarity with BSI Standard 200-2 and the IT-Grundschutz Compendium is a pre-requisite.

Note: The modernisation of IT-Grundschutz provides both more effort and the opportunity to revise thoroughly the existing security concept, to perform a critical review of previously implemented security safeguards, and to update and optimise these within the meaning of continual improvements.

3.1 Structure analysis

In comparison to the previous structure analysis in accordance with BSI Standard 100-2, the revised structure analysis (in accordance with BSI Standard 200-2) has changed predominantly with regard to business processes to which are now more in the foreground. The existing structure analysis results must be supplemented and entities much check whether the business processes that are within scope have been included in the structure analysis to the degree of precision necessary. If business processes have not been previously identified nor recorded clearly, nor linked to associated applications, this must be rectified based on the scope of the security concept. In addition, it makes sense to double-check identified applications as an application is useful within the structure analysis only if it is based on a business process. Of course, the structure analysis must be supplemented to include relevant service providers and any target objects within their spheres of influences (see requirements for outsourcing [OUT]).

In other regards, the existing structure analysis can continue to be used. In particular, applications, networks and IT systems should be checked and any results adopted. Please note that the modernised IT-Grundschutz more starkly differentiates between different types of IT systems, and considers industrial controlling systems (ICS) or other devices (e.g. Internet of Things) separately. If the information system has not undergone changes, entities must check whether assets previously covered under user-specific modules now have a corresponding module in the IT-Grundschutz Compendium. Finally, rooms, buildings and locations are recorded.

Action points:

- Identify relevant business processes within scope and include them in the structure analysis.
- Compare business processes with applications already listed and check whether all relevant business processes have been included in the structure analysis.
- Include service providers and all target objects within their spheres of influence if they are relevant to for the scope.
- Check and include any existing structure analysis.
- Check IT systems when recording them as to whether industrial controlling systems (ICT) and other devices are now covered under modules in the IT-Grundschutz Compendium.

The exact requirements and further information can be found in Section 8.1 of the BSI Standard 200-2.

3.2 Determining protection requirements

The methodology for determining protection requirements has changed mainly with respect to the basis used to determine the protection requirements: this is now business processes and associated information. Protection requirements determined for these elements is inherited any target objects used to process them, specifically applications, IT systems and ICS systems, and other devices (e.g. IoT devices), rooms and communications connections. In the past, the relevant applications were frequently used as the starting point for determining protection requirements. The protection requirements for applications must now be able to be derived consistently from the protection requirements of the business processes.

In other regards, the existing determination of protection requirements can be checked and adopted. This includes checking and adopting the categories of protection requirements and the protection requirements determined for IT systems, rooms, buildings and locations, and for communications connections. To the extent that both IT systems and industrial controlling systems (ICS) and other devices (e.g. IoT devices) have been determined in the structure analysis, protection requirements must be derived for these as well. When determining requirements, dependencies and inheritance rules must still be considered in terms of maximum, cumulative and distribution effects. What is more, the protection requirements also include the relevant protection objectives (confidentiality, integrity, availability). In addition, Section 8.2.4 of BSI Standard 200-2 provides notes on determining protection requirements within the context of cloud computing and virtual environments.

Action points:

- Determine protection requirements for business processes and underlying information.
- Derive from this and provide reasons for protection requirements for applications.
- Derive from this and provide reasons for protection requirements for ICS or IoT systems; if listed in an applicable manner, the protection requirements for ICS can be determined separately).
- Check and adopt protection requirements for further assets (including rooms, buildings and communications connections), while providing reasons.

The exact requirements and further information can be found in Section 8.2 of the BSI Standard 200-2.

3.3 Modelling

Due to stark changes in the IT-Grundschutz Compendium in comparison with the IT-Grundschutz Catalogues, modelling, specifically the selection of relevant modules from different layers, must be repeated completely. However, the modelling methodology itself has not changed.

This means that all modules relevant for the information system must be selected during modelling. Section 8.3 of the BSI Standard 200-2 and the IT-Grundschutz Compendium explain the methodologies orientated to the IT-Grundschutz layer model.

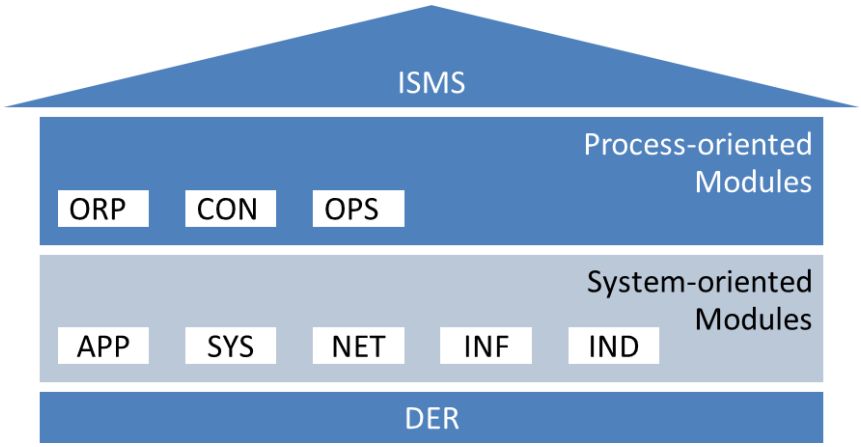

Figure 1: Layer model in accordance with IT-Grundschutz

German	English
Prozess-Bausteine	process-orientated modules
System-Bausteine	system-orientated modules

Next, we will initially turn to the process-orientated modules and then to the system-orientated modules:

Process-orientated modules:

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

System modules:

- The APP layer deals with safeguarding applications and services, among other things, in the areas of communication, directory services, network-based services and business and client applications. Typical modules of the APP layer are *General groupware*, *Office products*, *Web servers* and *Web browsers*.
- The SYS layer addresses the individual IT systems of the information system that may have been divided into groups. Here, the security aspects of servers, desktop systems, mobile devices and other IT systems such as printers and telecommunication systems are addressed. The SYS layer includes, for example, modules for concrete operating systems, Smartphones/tablet and Printers, copiers and all-in-one devices.
- The IND layer deals with the security aspects of industrial IT (ICS). This layer includes, for example, the modules *Machines*, *Sensors and actuators* and *Programmable logic controllers (PLC)*.

- The NET layer examines the networking aspects not directly related to specific IT systems, but to the network connections and the communication. This includes, for example, the modules *Network management*, *Firewall* and *WLAN operation*.
- The INF layer addresses the architectural and structural factors; here, aspects of infrastructural security are brought together. This concerns, among other things, the modules *General building* and *Computer centre and Server room*.

The result is a model that includes all modules of the Compendium and in which each module specifies the target objects for which and to which it can be applied. If a module cannot be used, a reason must be provided.

Section 2.2 of the IT-Grundschutz Compendium provides information on whether a module is to be used at a global level for once for an information system, or whether it is to be used multiple times. In addition, Section 8.3.5 of BSI Standard 200-2 provides notes on modelling within the context of virtualisation and cloud computing. In Section 8.3.7 of the BSI standards, you will find requirements for including external service providers (see also [OUT]).
As before, the requirements of the modules may be adjusted in line with the specific situation.

Action points:

- Carry out modelling in accordance with Section 8.3 of BSI Standard 200-2, also checking whether all modules can be used, assigning target objects and providing reasons for selection or non-selection.

The exact requirements and further information can be found in Section 8.3 of the BSI Standard 200-2 and in the IT-Grundschutz Compendium.

3.4 IT-Grundschutz check

The comprehensive content changes in the IT-Grundschutz Compendium and the paradigm shift that has taken place make it necessary to perform a completely new IT-Grundschutz check. These changes and shifts mean that entities must define specified safeguards, requirements and how they intend to fulfil them.

As mentioned, the recommended methodology is to perform a completely new target-actual comparison and to record the following information for each layer, each module selected and each requirement:

- Implement the safeguard, i.e. describe which safeguards at the entity meet the requirements.
- Specify the status of the implementation of the safeguard.

BSI supports users in this comprehensive documentation process using its ‘migration tables’, which illustrate the relationship between requirements from new IT-Grundschutz modules and previous safeguards from the classic IT-Grundschutz. This allows an entity to initially determine which existing safeguards have been assigned to a requirement and to then check whether these implemented safeguards meet the new requirement in each case. These safeguards to meet requirements and the status of implementation must be documented in each case.

Often, the definition of safeguards (to meet a requirement) goes hand in hand with the description of the safeguards implemented in the case of an established ISMS. Despite this, this process should still be critically reviewed as to whether a safeguard is sufficient to meet the requirement.

If safeguards implemented to date are not sufficient for a requirement, an entity must first define additional safeguards and categorise its implementation status with "no" or "partially". This requirement and its associated safeguards must then be adopted into the risk management plan and processed there. An audit and certification process (see [BSI2002]) governs how to handle safeguards that have not been fully implemented.

At entities which have already maintained detailed documentation for each safeguard specified, how the concrete safeguards were implemented and where the "Comments/Reason for not implementing" field has been used, will find this migration process considerably easier to manage.

With regard to establishing a relationship between safeguard and requirement, different cases can be found:

- Some requirements may be able to be modelled using existing safeguards. In these cases, implementation is relatively easy to achieve.
- By contrast, there are some requirements that cannot be modelled using the safeguards for an original module. Instead, the individual safeguards from other modules must be analysed. In these cases, implementation is also relatively easy.
- Of course, there are new requirements for which safeguards must first be defined and then for which the implementation status must be documented.

See Section 4.3 of this document for more information on the migration tables. Other resources include tools that entities use to document their ISMS (see Section 4.2).

Action points:

- Process each individual requirement of the module for each layer and each module of the model as follows:
  - Define and document safeguards to meet the requirement. Migration tables are resources for quickly identifying the corresponding requirement to which an existing safeguard corresponds. This can help to determine the situation documented currently.
  - Check whether safeguards are sufficient for meeting the requirement.
  - Check and document the status of implementation of the defined safeguard (yes, partially, no).
  - Include in the risk management plan any requirements and their associated safeguards that are not implemented or only partially so.

The exact requirements and further information can be found in Section 8.4 of the BSI Standard 200-2.

3.5 Risk analysis

A risk analysis is considered successful if there are target objects

- that have high or very high protection requirements in at least one of the three basic values of confidentiality, integrity or availability
- that cannot be adequately mapped (modelled) with the existing modules of IT-Grundschutz
- which are used in operating scenarios (environment, application) that are not planned in the scope of IT-Grundschutz

Assuming that one of these pre-requisites applies, the supplementary security analysis is no longer relevant to the previous IT-Grundschutz. Here, the following must be taken into consideration:

- If a supplementary security analysis has been performed previously and it was determined at management level that no further risk analysis was necessary, a risk analysis must now always be performed.

In this case, migration is not possible. Instead, a risk analysis, e.g. in accordance with BSI Standard 200-2 is required.

- By contrast, if the supplementary security analysis determined that a risk analysis was necessary for selected target objects only, a risk analysis must now always be performed for target objects excluded by the supplementary security analysis.
- In the case of all target objects for which a risk analysis was performed in accordance with the deprecated BSI Standard 100-3, BSI recommends updating the existing risk analysis.

To update the risk analysis, a risk analysis in accordance with BSI Standard 200-3 can be performed. In addition, the migration approach described in the following can be selected. Entities using another established method (e.g. ISO/IEC 27005, ISO/IEC 31000) or an adjusted methodology for analysis of information security risks may adapt the following recommendations correspondingly.

Migration to 200-3:

First, provide a list of target objects for which a risk analysis must be performed. The pre-requisites listed above apply. This overview is the starting point for the risk analysis and does not differ from the methodology in accordance with BSI Standard 100-2. To ensure that this task can be performed with reasonable effort, it is important that the target objects be consolidated into reasonable groups. If a risk analysis must still be performed for many target objects despite grouping them, priorities should be defined (see Chapter 2 of BSI Standard 200-3).

Then, the relevant elementary threats for each target object are collected and assigned to the target object. The risk analysis in accordance with BSI Standard 200-3 is now completely shifted to the elementary threats. The specific threats from IT-Grundschutz Catalogues (G1-G5) will no longer factor into future risk analyses. This means that all security concepts that are still based on specific threats must check existing risk analyses to determine whether they are still applicable to the current threat situation and all whether all elementary threats were analysed.

Entities which have already migrated to elementary threats may use their existing analyses and update the list of relevant threats. Please take special care to also analyse the threat overviews of the IT-Grundschutz Compendium (lists of the relevant elementary threats are cross-referenced in a table of modernised modules).

In addition, further threats may be included. This methodology underlying this step has not changed, meaning that previous information can be used for the analysis.

After identifying target objects and relevant threats, risk is analysed with the following steps:

- risk estimate specifying frequency of occurrence and extent of damage
- risk assessment – BSI Standard 200-3 provides a sample matrix approach with various risk categories. This replaces the previous evaluation (based on the checking criteria of completeness, mechanism strength, reliability) of whether or not implemented safeguards or safeguards planned in the security concept are sufficient ("OK=Y" or "OK=N")
- risk management with typical options depending on the entity's risk appetite:
  - risk avoidance by changing the scope
  - risk reduction by implementing additional security safeguards
  - risk transfer by purchasing corresponding insurance policies
  - risk acceptance by adopting residual risk

As before, management must still approve any residual risk that must be accepted. Also unchanged is how to handle additional safeguards that must flow back into the security concept.

As part of the result, an entity must determine whether the methodology used to perform risk analyses has changed significantly. It is therefore important to adjust the entity's guidelines for performing the risk analysis. In particular, the selected methodology, estimates, assessments and management of risks, and risk acceptance criteria must be defined in advance of the risk analysis.

Action points:

- Identify target objects for which a risk analysis must be performed. Consider only these target objects (analysed target objects) in depth.
- Identify target objects for which the supplementary security analysis determined that no further risk analysis was necessary.
- Perform a risk analysis for these target objects in accordance with BSI Standard 200-3 (migration is not possible in this case).
- Migration is possible for target objects for which a risk analysis has always been performed in the past:
  - Check and adopt list of relevant target objects.
  - The relevant threats must be either collected and assigned to target objects or the their target object assignment must be check and adopted.
  - Either perform or check and adopt the risk estimate for each target object while taking into consideration its frequency of occurrence and extent of damage.
  - Either perform or check and adopt the risk assessment for each target object.
  - Either perform or check and adopt the risk management for each target object.
  - Management must approve acceptance of residual risk.
  - Integrate additional security safeguards into the security concept, possibly by creating a user-defined module.

The exact requirements and further information can be found in BSI Standard 200-3.

4 Resources

4.1 Implementation recommendations

There are implementation recommendations for many modules of IT-Grundschutz, including sample recommendations for security safeguards for implementing the module requirements. These are based on best practices and long-term experience of information security experts. However, the safeguards of the implementation recommendations are not considered binding. Instead, they can and should be supplemented or replaced by entity-specific safeguards.

4.2 Tools

Several providers have a series of tools that support security concepts in accordance with IT-Grundschutz (see [GST]). These tools will support the migration from the previous IT-Grundschutz to the current version. The specific functions offered by each tool is dependent on the particular product.

The following information on "automatic" migration must be taken into consideration:

- Tool offering a migration function support the process and likely reduce onerous documentation tasks.
- At the same time, it is important to remember that ISMS is a process, not a product. While the possibility of migrating to the modernised IT-Grundschutz at the touch of a button is certainly tempting, entities should seize the opportunity to thoroughly review their ISMS and develop it further within the meaning of the PDCA cycle (plan, do, check, act) on an ongoing basis. This is how to ensure that new features of the modernised IT-Grundschutz take full effect (new, updated modules and new degrees of freedom in selecting safeguards to meet requirements).

4.3 Migration tables

When modernising IT-Grundschutz, the existing modules of the IT-Grundschutz Catalogues were converted into the new format. Specifically, a migration table was created for each migrated module. This table maps how requirements (IT-Grundschutz Compendium) are assigned to security safeguards (IT-Grundschutz Catalogues). These tables from BSI provide comprehensive information to ensure a smooth, efficient transition.

The IT-Grundschutz check uses migration tables to easily determine which previous safeguards correspond to each corresponds. This allows users to determine the previous safeguard that corresponds at least when selecting the appropriate safeguard to meet the requirement. However, there is not always a 1:1 relationship between the (new) requirements and (old) safeguards, meaning the old safeguard cannot always be adopted as a new requirement. The migration tables are structured as followed:

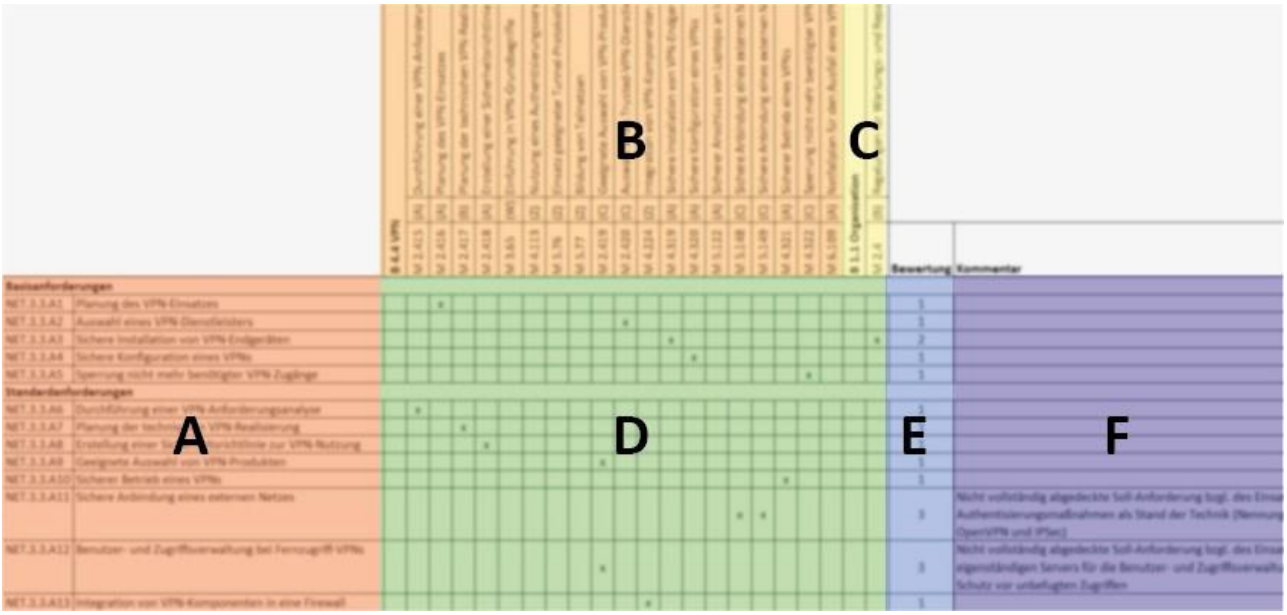

Figure 2: Migration table structure

- At left under each other, you will see all basic and standard requirements and the requirements where protection requirements are higher, i.e. for the (new) modules of the IT-Grundschutz Compendium (Section A in the figure).
- The safeguards of the (old) modules of the IT-Grundschutz Catalogues are shown above. The list always begins with the original module of the 15th supplement delivered, which best matches the new module from the IT-Grundschutz Compendium (Section B). Below this are any safeguards from secondary modules (Section C). As a rule, however, only context-specific modules have been taken into account. For example, this means in the case of the NET 1.1 module *Network Architecture and Design* that no safeguards from the old module B 3.101 *General Servers* have been referenced, even if some individual sections would fit.
- Under this are the assignments, marked with an "x". An "x" means that there is related content between this requirement ("new") and the corresponding safeguard ("old") (Section D).
- To the right, the type of relationship is shown with the specified assessment using the digits 1, 2 or 3 (Section E). The following situations must be differentiated:
  1. The requirement is fully covered with the safeguards from the corresponding module in the 15th supplemental delivery (SD). If the safeguard(s) were previously implemented in full, no further revision of the requirement is mandatory.
  2. The requirement is fully covered only when additional safeguards from other modules of the 15th SD are taken into account. A check must be performed as to whether full coverage is actually necessary because the safeguards are sourced from a different context (module). This assessment is still taken, even if the safeguard from the 15th SD is only a recommendation or for informational purposes. The comment field contains a relevant note.
  3. The requirement is not fully covered in every case under additional safeguards from the 15th SD. An in depth check must be performed to determine how the requirement can be met. The comment field contains a relevant note about possible areas not covered by the requirement.
- The comment field is to the right of the assessment (Section F).

The following framework conditions and notes must be observed when using this:

- All requirements are treated the same as an individual check must be performed if there is any doubt.
- That other safeguards from modules outside the 15th SD may fit, rather than only the safeguards identified in the migration tables, cannot be excluded.
- If requirements cannot be covered under safeguards from the original module, potential references to other modules will be provided. These are to be understood as tips and must be checked manually by users.
- While the content of the original safeguards were adopted to a large degree for the modernisation when the requirements were put together, marginal changes have been made (e.g. stricter requirements). For example, safeguard M 2.322 *Determining a Security Policy for the Client-Server Network* from the module of the same name in B 3.201, *General Client* provides nearly full coverage of the SYS.2.1.A9 requirement *Determining a Security Policy for Clients*. At the same time, this was supplemented by the documentation obligation of the regular implementation check: "The implementation of the contents required in the policy SHOULD be checked at regular intervals. The results SHOULD be documented in a reasonable manner." In these cases, assessment 3 was taken and there is a corresponding note in the comment field.

These three examples are intended to clarify how the migration tables should be used.

Example 1: modules that are essentially the same

Some modules adopted were not changed essentially, for example NET.3.3 *VPN*. As can be seen in the associated migration table, the requirements of the "new" module NET.3.3 *VPN* are covered largely by the "old" modules B 4.4 *"VPN"* and B 1.1 *Organisation*. If the safeguard(s) were previously implemented in full, no further revision of the requirement is mandatory.
The requirement is considered to be implemented and the text from the "old" basic security check can be adopted into the new IT-Grundschutz check. The NET.3.3.A3 requirement *Securing Installation of VPN End-User Devices* is implemented fully only when taking into account M 2.4 *Rules of Maintenance and Repair Work* from module B 1.1 *Organisation* , meaning one can also consider this requirement to have been implemented. A check must still be performed.

Example 2: modules for which the content has changed

Some modules have the same name, but their content has been extensively revised, for example SYS.2.3 *Clients under Unix*.

The associated migration table shows that assignment to the old module of B 3.204 *Clients under Unix* overlap only to a very basic degree in content, as the old module was the 2009 version. Very few requirements can be covered fully by the old safeguards. Assessment 3 for the majority of requirements does not, however, necessarily mean that they must also be implemented by users. It means generally that the specific requirement was not included in the previous module. For example, SYS.2.3.A19 defines the requirement of hard drive encryption using certain methods or tools. This aspect was not analysed to this degree of detail in the 15th SD. Users must take into account individually any references to potential safeguards from the 15th SD, as to whether these requirements have already been implemented.

Example 3: new modules

Lastly, some modules are completely new. This includes APP.1.1 *Office Products* or SYS.3.2.2 *Mobile Device Management (MDM)*. There are no migration tables in this case. However, a check should be performed as to whether user-defined modules existed for these areas. Such modules should be compared with the new modules.

There will still be areas that the IT-Grundschutz modules do not cover. If an entity has developed user-defined modules, it is useful to share these with BSI, which will then make them available to the IT-Grundschutz community. BSI will anonymise any modules provided, if desired, or give credit to the authors.

Note: Migration tables are a very sophisticated way to map the many changes made. Despite intensive quality controls, they could still contain errors. If you find any, please notify us via the IT-Grundschutz hotline:grundschutz@bsi.bund.de.

References

[27005] ISO/IEC 27005:2011 "Information technology - Security techniques - Information security risk management", ISO/IEC JTC 1/SC 27, 2011

[31000] ISO/IEC 31000:2009, "Risk management – Principles and guidelines", ISO/TC 262, 2009

[AUD] Certification in accordance with ISO 27001 on the basis of IT-Grundschutz, Auditing Scheme, Federal Office for Information Security (BSI), Version 2.0, October 2017

[BSI1001] Information Security Management Systems (ISMS), BSI Standard 100-1, Version 1.5, May 2008

[BSI1002] IT-Grundschutz Methodology, BSI Standard 100-2, Version 2.0, May 2008

[BSI1003] Risk Analysis on the Basis of IT-Grundschutz, BSI Standard 100-3, Version 2.5, May 2008

[BSI2001] Information Security Management Systems (ISMS), BSI Standard 200-1, Version 1.0, May 2017

[BSI2002] IT-Grundschutz Methodology, BSI Standard 200-2, version 1.0, October 2017

[BSI2003] Risk Analysis Based on IT-Grundschutz, BSI Standard 200-3, Version 1.0, October 2017

[FRIST] Transitional Periods and Migration in the Context of Certification, Federal Office for Information Security (BSI), August 2017

[GSKO] IT-Grundschutz Compendium, BSI, published annually, https://www.bsi.bund.de/grundschutz

[GSM] Modernising IT-Grundschutz, BSI, https://www.bsi.bund.de/gs-modernisierung

[GST] Alternative IT-Grundschutz Tools, BSI, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GSTOOL/AndereTools/anderetools_no_de.html

[OUT] IT-Grundschutz Methodology in the Context of Outsourcing, Federal Office for Information Security (BSI), Version 1.0, October 2017

[PRUEF] Basis for Checking Certifications in Accordance with ISO 27001 on the Basis of IT-Grundschutz, Version 3.1, February 2018

[ZERT] Certification in accordance with ISO 27001 on the basis of IT-Grundschutz, Certification Scheme, Federal Office for Information Security (BSI), Version 2.0, September 2017