Bundesamt
für Sicherheit in der
Informationstechnik

IT-Grundschutz Profiles - Structural Description -

COMMUNITY DRAFT

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

Change history

Version	*Date*	*Name*	*Description*
0.1	22/01/18	BSI	Community Draft

1 Introduction

This structural description provides an overview of how an IT-Grundschutz profile is structured. For the purposes of clarity, each section includes an example (in blue font) which could also be used in this form in a profile for E-commerce providers.

Motivation

The cyber threat situation poses new challenges for information security through increasingly professional and sophisticated attacks. Each organisation must create an individual security concept for its internal requirements in order to minimise the risks involved. Depending on which IT-Grundschutz methodology an organisation has chosen, it will need to determine a number of framework conditions to enable the introduction to the actual security process. This includes, for example, identifying existing business processes and specialist tasks, IT systems, applications, rooms and communication links, determining the protection requirements, modelling modules, performing an IT-Grundschutz check, and conducting a risk analysis under certain circumstances. IT-Grundschutz profiles can be used to address these steps in advance in a generalised manner for specific application areas, which enables organisations to continue to work on these samples and thus save a lot of work and time.

Objective of IT-Grundschutz profiles

The objective of IT-Grundschutz profiles is to offer sample scenarios for certain application areas, which facilitate individual users in these areas when mapping the security process according to IT-Grundschutz to their individual framework conditions. An IT-Grundschutz profile is a template for a selected scenario (information system or business process) via which the IT-Grundschutz implementation is specified for this area. An IT-Grundschutz profile is used to prepare various steps of the information security process for a defined application area in such a manner that it can be adapted as a framework for security concepts. These steps include the following:

- Specifying the application area
- Implementation of a generalised structure analysis, determination of protection requirements and modelling process for this area
- Selection and adaptation of IT-Grundschutz modules to be implemented
- Description of specific safety requirements and safeguards as well as
- risk analysis and risk handling if necessary

In order to identify the relevant requirements and appropriate security recommendations for a specific application area and to map them in an IT-Grundschutz profile, they should be created in collaboration with representatives of the future users. Thus profiles should be created by committees or user groups of an industry or by representatives of a subject area, supported by the IT-Grundschutz team of the BSI.

Profiles should subsequently be made available to the interested community. This enables experience and expertise to be shared and benefits to be derived from synergy effects. Within

an individual organisation, the persons responsible for information security can focus on implementing specific security recommendations in future. All organisations involved can benefit from the time saved as well as the human and financial resources that are spared. The new IT-Grundschutz profiles may be used in the following application areas, among others:

- local authorities
- hospitals or
- waterworks as critical infrastructure.

The IT-Grundschutz profiles created by one or more organisations in a particular industry or by an association can be integrated by other users into their security concepts.

Individual business processes or specialist tasks can also be mapped on the basis of IT-Grundschutz profiles, in addition to security concepts for information systems. Examples within the area of public administration include procedures such as the “Nationale Waffenregister” (NWR - German Arms Register) or the “electronic files”.

Advantages

IT-Grundschutz profiles offer the advantage of enabling committees to provide their users with a tool box that has already been adapted to their specifics, their terminology and their background knowledge. Depending on the security requirements for the area under consideration, the necessary components of the IT-Grundschutz can be compiled in a modular manner. As a result, security concepts in an industry are not only easier to create, but are also more comparable.

Objective of this document

The basic structure of IT-Grundschutz profiles is described in this document. In addition, an exemplary presentation of the Reference Architecture of E-commerce providers shows how individual structural elements of an IT-Grundschutz profile might look in practice. Examples within the document are highlighted via a blue font colour.

2 Structure of IT-Grundschutz Profiles

The manner in which an IT-Grundschutz profile should be structured is presented below. The structure shown is useful for ensuring that no aspects are forgotten and facilitates comparability as well as recognition by the BSI. Depending on the deployment scenario or purpose, however, the structure of a profile can also deviate from it.

IT-Grundschutz profiles should have the following structure:

- Formal aspects (publisher, registration number, version, duration)
- Management summary
- Scope
- Relevant modules, requirements and safeguards
- Assessment of residual risks/risk handling
- Notes on Application
- Supporting information
- Appendix

2.1 Formal aspects

The first section of the IT-Grundschutz Profiles gives an overview of basic formal aspects. The following points should be described at least:

- Title (short title):

  Full title of the profile, a memorable short title can be added within brackets.

- Author:

  Persons or organisations that have created the IT-Grundschutz profile. They may include, for example, consultants who have been commissioned to create the profile. Individual project participants may also be named here.

- Publisher:

  Specification of the industry, the committee or the work group

- Registration number:

  Unique identifier, consisting of an identifier for IT-Grundschutz profiles as well as an annually continuous and unique number. The registration number can be used to uniquely reference the IT-Grundschutz profile.

- Version:

  In addition to a registration number, each IT-Grundschutz profile is also assigned a version. This enables users to see when the IT-Grundschutz profile was generated or updated and when it was last reviewed.

At least: publication status, version number, date of creation. For established and already published documents: date of last change, date of last review

- Revision cycle:

Indication of the interval after which the document should be reviewed to assess its up-to-dateness

- Confidentiality:

  Here, it is also possible to enter whether the IT-Grundschutz profile is open or confidential (and thus only accessible to certain users).

  A classification, for example, according to TLP (Traffic Light Protocol) or VSA (instructions for the handling of classified information) is possible here.

- Recognition by BSI:

  Information including status as to whether the profile was or should be recognised by the BSI.

Example: Formal aspects

Title:	Electronic commerce over the Internet (eCommerce)
Author:	BSG
Publisher:	AK eCom
Registration number:	GS-PRO_2017-0001
Version:	Working Draft, Version 1 of 07/02/2017
Revision cycle:	annually
Confidentiality:	public
Recognition by BSI:	recognition is still being discussed

2.2 Management summary

The actual introduction to a profile starts with a management overview in order to present the objective of the IT-Grundschutz profile within a few lines for readers with limited time. From the short overview, the management should already be able to see which core statements are contained in the IT-Grundschutz profile. The underlying target group is also described here. Furthermore, the initial recommendations for action and decision-making (based on risk handling) can also be integrated within the management overview, and the most important residual risks should be visible at first glance.

The following aspects should be summarised in a management overview:

- Brief description of the target group addressed
- Brief description of the objective
- Management tasks (brief description of recommendations for action and decision-making, e.g. based on the risk handling results)

Example: Management summary

Target group

This IT-Grundschutz Profile is orientated to E-commerce providers that offer online products and/or services and which, as a result, regularly work with customer data.

Objective

It defines a minimum protection requirement for the thus processed personal data, payment transaction data as well as for the E-commerce offer. In addition to the modules to be applied in accordance with the IT-Grundschutz methodology “standard security”, the profile includes a specific “E-payment” module as well as additional individual requirements.

The BSI recommends that E-commerce providers use this profile as the basis for their security concept.

2.3 Definition of the scope

The scope contains an exact description of what the IT-Grundschutz profile covers, i.e. the type of business processes and information systems for which the profile is suitable. This includes at least one paragraph in each case on the following aspects:

- Description of the target group to which this profile is addressed
- Description of the underlying protection requirements, including an explanation
- Description of the basic IT-Grundschutz methodology on which the creation of the profile is based, together with the extensions or restrictions to be considered in relation to the IT-Grundschutz methodology described in BSI standard 200-2

The following points should also be listed:

- Cover approach:

  Statement as to the level of protection achieved with the IT-Grundschutz profile compared to the IT-Grundschutz methodology

- ISO 27001 compatibility:

  Furthermore, an overview of its compatibility with other information security standards (e.g. ISO/IEC 27001:2013) should be provided. If at least the IT-Grundschutz methodology “standard security” is implemented, it is compatible with ISO 27001. In the event of a lesser degree of meeting of requirements than under “standard security”, the creator of the IT-Grundschutz profile must check the compatibility if necessary.

- Framework conditions:

  Listing of framework conditions (e.g. legal bases) or compliance requirements on which the IT-Grundschutz profile is based.

- Compliance obligation (optional)

  There may be a description as to whether the profile is of a mandatory or recommended nature for the target group.

Example: Definition of the scope

Target group

This IT-Grundschutz Profile is orientated to e-commerce providers who offer online products and/or services and who regularly work with customer data as a result.

Protection requirements

In terms of the level of protection, this profile defines a level that exceeds the standard security of the IT-Grundschutz methodology since E-commerce services usually involve the processing of large volumes of personal customer data with huge importance attached to its confidentiality. Furthermore, there is usually an increased protection requirement with respect to the availability of the services offered by the E-commerce provider. Thus a protection requirement of "high" is to be assumed with respect to the confidentiality and integrity of personal customer data and payment transaction data. An availability requirement of "high" is to be assumed for an E-commerce offer. This assessment of protection requirements is to be considered when using the IT-Grundschutz profile.

IT-Grundschutz Methodology

The requirements listed in this profile are recommendations of the AK eCom for E-commerce providers. They cover at least the requirements of the “standard security” of BSI standard 200-2, and requirements from the area of high protection requirements must also be implemented in some instances.

Cover approach:	Minimum standard, high in some instances
ISO 27001 compatibility:	Yes
Framework conditions:	**The requirements presented in this profile consider the requirements of the Federal Data Protection Act (BDSG) and Section 13 of the German Telemedia Act (TMG).**

2.4 Definition of the information system

It is necessary to clearly define the information system or business process/specialised task under consideration. This includes statements about what is or what is not the subject of the profile. The following aspects should be specifically described:

- Components of the information system or of the business process/specialised task
- Objects not considered: Reasons must be provided if target objects relating to the information system are not considered in the profile.
- Connection to other IT-Grundschutz profiles

Example: Definition of the information system

Components of the information system

The “E-commerce” information system includes all processes and procedures of an E-commerce provider that are necessary for the completion of online transactions. At the technical level, the website, databases, e-mail and other communication servers and the

corresponding network infrastructure are usually included as well as other IT systems that are essential for the E-commerce offer.

Objects not considered

The clients used by the E-commerce provider's employees for office communication are not considered by the IT-Grundschutz profile because they are not essential for the E-commerce offer.

E-commerce providers who allow a large part of their technical infrastructure to be operated by third parties should use this profile as the basis for selecting appropriate service providers. The requirements formulated here should be included in the terms of the contract.

Reference to other IT-Grundschutz profiles: not applicable

2.5 Reference Architecture

The Reference Architecture (subject under examination) determines to which objects the requirements of IT-Grundschutz must be applied in the context of the IT-Grundschutz profile. In addition to business processes, this may include infrastructure elements such as buildings and rooms, as well as the relevant IT systems with the installed applications. They can be displayed in an overview and a network plan (see Figure 1). For complex information systems, it may be useful to consider only a subsection of the information system with the IT-Grundschutz profile. The entire information system can then be mapped with other separate IT-Grundschutz profiles for individual sub-systems.

The following relevant objects should be listed with a unique identifier and a short description. Ideally, they should be grouped into object groups or depending on the identified business processes:

- Infrastructure: buildings and rooms
- Networks and communication: networks, network components and communication links
- IT systems (servers, desktop systems, mobile devices, etc.)
- Business processes / applications

In order to reduce complexity, similar target objects should be grouped together.

If necessary, the manner in which deviations and extensions to the Reference Architecture can be dealt with should also be described. This is important if the actual infrastructure elements, IT systems and applications, or business processes or specialist tasks differ from the Reference Architecture. These deviations should not be too large since it would then be more useful to generate a separate profile, for example, based on this IT-Grundschutz profile.

Example: Reference Architecture

The information system considered by the IT-Grundschutz profile considers all essential objects of the E-commerce provider and is described in the following section "Subject under examination".

Subject under examination

Infrastructure:

- [R1] Buildings
- [R2] Server room
- [R3] Workplace for administration and configuration

Networks and communication

- [K1] ISP connection
- [N1] Separated LAN
- [N2] Active network components (routers, switches)
- [N3] Security components (firewall, multiple packet filters)
- [N4] Management network (out-of-band)

IT systems:

- Communication server:
  - [S2] E-mail server
- Three-layer architecture of the online offer comprises:
  - [S3] Web server to display the E-commerce website
  - [S4] Application server for the execution of the E-commerce application
  - [S5] Database server for reserving persisted e-commerce data, including customer data
- Payment system
  - [K2] VPN connection to payment transaction service provider
  - [S1] VPN server
- [S6] Payment server for payment system
- [C1] IT system for administration and configuration of networks and IT systems

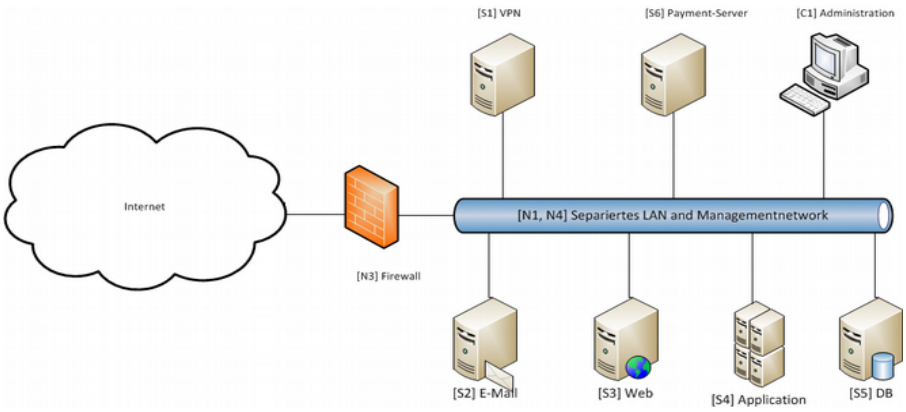

Figure 1: E-commerce network plan

Handling deviations
If the information system to be protected differs from the Reference Architecture, the additional or unavailable objects must be documented. They are to be assigned to suitable modules of the IT-Grundschutz Compendium. The requirements derived from the modules must be adapted depending on the protection requirements.

2.6 Requirements to be met and safeguards to be implemented

It can be specified in an IT-Grundschutz profile whether all requirements of a module or only a selection, such as only the basic requirements or additionally selected standard requirements, are relevant. Furthermore, the selected requirements can and should be specified. Not only existing requirements from the IT-Grundschutz modules can be assigned to the profile, but also requirements that have not existed as yet in the IT-Grundschutz. This enables the IT-Grundschutz profiles to be used to achieve a security level that corresponds exactly to the protection requirements of the considered application area. This can then cover basic security, standard security or increased protection requirements.

Assigning relevant modules

Once the Reference Architecture has been defined and the relevant target objects have been identified, the next central task involved in the creation of an IT-Grundschutz profile is to reproduce the considered information system (subject under examination here) by means of the IT-Grundschutz model. For this purpose, existing modules are selected and implemented in the IT-Grundschutz Compendium (also see BSI standard 200-2, Section 8.3 Modelling an information system or Section 2 of the IT-Grundschutz Compendium). In order to facilitate selection, the modules of the IT-Grundschutz Compendium have been divided into process-oriented and system-oriented modules. Process-oriented modules deal with comprehensive security aspects that apply equally to all or large parts of the information system (e.g. ORP.1 Organisation or ORP.2 Personnel). System-oriented modules, on the other hand, address security aspects of specific components (e.g. IT systems (SYS.1.3 Unix server) or applications (APP.3.2 Web server)) and can thus be modelled on relevant objects of the Reference Architecture.

The IT-Grundschutz Compendium contains security requirements for typical business processes, applications, and components. Under certain circumstances, a target object cannot be mapped or cannot be sufficiently mapped with the existing modules from the IT-Grundschutz Compendium. In such cases, a risk analysis must be carried out on the considered target object (also see BSI standard 200-3 risk analysis based on IT-Grundschutz).

This step results in a list or table that lists the modules that are relevant to the underlying Reference Architecture. As described above, the process-oriented modules are important for many target objects, while the modules in the other layers (see the layer model of the IT-Grundschutz Compendium) refer, on the other hand, to specific target objects or groups of target objects that are included in the Reference Architecture.

Relevance of requirements

After the relevant modules of the IT-Grundschutz Compendium have been identified, the next step in creating IT-Grundschutz profiles is to adapt the requirements according to the target group. The modules include suggested requirements that are typically suitable and appropriate for these components. In order to create an IT-Grundschutz profile, it is necessary to work through the individual requirements and adapt them, if necessary, to the framework conditions of the profile.

It may be useful, for example,

- to identify all requirements of a module as relevant,
- to identify only certain requirements as relevant (e.g. basic requirements only),
- to specify requirements, for example, to supplement other aspects, or
- to discard requirements completely.

It is not only existing requirements from the IT-Grundschutz modules that can be assigned to the profile, since it is often necessary in practice to identify further requirements beyond those in the IT-Grundschutz modules, which are of importance for the information system under consideration. This is the case, for example, if there are increased protection requirements or if individual target objects of the Reference Architecture cannot be mapped or cannot be sufficiently mapped with the existing modules from the IT-Grundschutz Compendium.

This enables the IT-Grundschutz profiles to be used to achieve a security level that corresponds exactly to the protection requirements of the considered application area.

This step results in a list or table that lists the requirements that are relevant to the underlying Reference Architecture. It must be noted that this list also includes the additional security requirements that have arisen from the risk analysis and which go beyond the IT-Grundschutz model (e.g. requirements for increased protection needs or requirements from user-defined modules).

Relevance of the safeguards (<implementation requirement>)

The requirements contained in the IT-Grundschutz modules describe what should be done. Users can choose different ways of meeting them, such as those described in the safeguards in the implementation information for the modules. The IT-Grundschutz profiles can be used to define how the requirements must be met in the context of the IT-Grundschutz profile. As responses with respect to meeting the individual requirements <implementation requirement>, the following statements are possible:

- “In an appropriate manner”: The decision as to how the requirements can be met is at the user's discretion.
- “By implementing the corresponding safeguards of the implementation information”: The safeguards of the implementation information must be implemented to meet the requirements.
- "By implementing [...] ": The safeguards for implementation can be found in other sources to which reference can be made. A safeguard can also be specified directly.

Although a specification as to how the requirements must be implemented enables a uniform meeting of requirements, it may be more useful to dispense with a relevant implementation requirement in the context of an IT-Grundschutz profile.

Implementation requirements of individual modules

After identifying all relevant modules and the general requirements and safeguards to be met, the extent of meeting the requirements and a specification for implementation can be defined for each individual module as follows:

- Dispensing with (individual) standard requirements:
  All basic requirements must <implementation requirement> be met.

All standard requirements must <implementation requirement>be met except for the following standard requirement:

    - Specification of the corresponding standard requirements of the module, which do not have to be met in the context of the profile, with valid justification (risk assumption, risk reduction by meeting alternative requirements, risk transfer)

- Mandatory meeting of requirements for increased protection needs
  The following requirements for increased protection needs should <implementation requirement> also be met:

    - Specification of the corresponding requirements with increased protection needs of the module through optional <implementation requirement>

- Additional requirement: *The following requirements must be met <implementation requirement> in addition to the module requirements*:

    - Additional requirement and description through optional <implementation requirement>

- Mandatory specification of a safeguard to meet a requirement:
  The requirements of the module must be met or supplemented by the following safeguards:

    - Specification of the requirement by implementing [...]

- Conditional restriction for application of a module:
  It is possible to dispense with meeting the requirements of the module if [...]

Example: Requirements to be met and safeguards to be implemented

The following obligatory **process-oriented modules** must be applied to the entire information system. Unless otherwise stated, all basic and standard requirements of the modules must be met *in an appropriate manner*:

- ISMS.1 ISMS (Security management)

    - The following requirements for increased protection needs must also be met by implementing the corresponding safeguard of the implementation information:

        - ISMS.1.A15 Creating target-group-oriented security policies

        - ISMS.1.A17 Taking out insurance
- ORP.1 Organisation
- ORP.2 Personnel
    - All basic requirements of the module must be met appropriately.
    - All standard requirements must be met appropriately except for the following standard requirement:
        - ORP.2.A10 Avoiding factors impairing the work climate

      Rationale:
        - Due to an almost family-like and friendly corporate structure, no additional requirements have to be met for a positive work climate.
- ORP.3 Information security awareness and training
- ORP.4 Identity and access management
- ORP.5 Requirements management (compliance)
- CON.1 Crypto-concept
    - The requirements “CON. 1. A9 Selection of cryptographic products" of the module are to be met or supplemented by the following safeguards:
        - “Use of hardware security modules”: Hardware security modules should be used to encrypt personal data, credit card data and other payment data.
    - The requirement “CON.1.A19 Encryption of data media” of the module must be met or supplemented by the following safeguards:
        - “Full encryption of business-critical data media”: All data media that contain business-critical, personal or financial data should be fully encrypted, at least with AES-256.
- CON.2 Data protection
- CON.6 Deleting and destroying
- OPS.1.2.1 Change management
- OPS.1.2.2 Archiving
- OPS.1.2.7 Sale/disposal of IT
- DER.1 Detection of security incidents in IT
- DER.2.1 Handling security incidents
- DER.3 Security checks
- DER.4 BCM/Business continuity management
- OPS.1.1: Core IT operations / core tasks
    - The requirements of the module do not need to be met if the IT infrastructure is operated by third parties

- OPS.2.1 Outsourcing usage
    - The requirements of the module do not need to be fulfilled if the IT infrastructure is self-operated
- OPS.2.5 SLA/SSLA
    - The requirements of the module do not need to be fulfilled if the IT infrastructure is self-operated

Additional requirements that must be met for the entire information system:

- The requirements of the BSI publication “Absicherung von Telemediendiensten nach Stand der Technik” (Securing Telemedia Services According to the State of the Art) must be met by the recommendations specified in the publication.

Furthermore, all modules are to be implemented, which result from the application of the IT-Grundschutz methodology, especially the modelling of the information system.

The following mandatory **system-oriented modules** are to be applied to the target objects (see Reference Architecture) specified in square brackets. Unless otherwise stated, all basic and standard requirements of the modules must be met *by implementing the corresponding safeguards of the implementation information*.

Infrastructure

- [R1] Buildings
    - INF.1 General building
    - INF.4 IT cabling
- [R2] Server room / technology room
    - INF.5 Server room / technology room
- [R3] Workplace for administration and configuration
    - INF.8b Office workplace

Networks and communication

- [K1] ISP connection
    - NET.1.1 Network architecture and design
    - NET.1.2 Network management
- [N1] Separated LAN
    - NET.1.1 Network architecture and design
    - NET.1.2 Network management
- [N2] Active network components (routers, switches)
    - NET.3.1 Routers / switches
- [N3] Security components (firewall, multiple packet filters)
    - NET.3.2 Firewall
    - NET 3.4 IDS/IPS

- [N4] Management network
    - NET.1.1 Network architecture and design
    - NET.1.2 Network management

IT systems:

- Communication server:
    - [S2] E-mail server
        - SYS.1.1 General server
        - SYS.1.3 Unix server (or similar module)
        - APP.5.1 E-Mail / Groupware
- Three-layer architecture of the web offer comprises:
    - [S3] Web server to display the E-commerce offer
        - SYS.1.1 General server
        - SYS.1.3 Unix server (or similar module)
        - APP.3.2 Web server
    - [S4] Application server for the execution of the E-commerce application
        - SYS.1.1 General server
            - The following requirements must be met in addition to the module requirements:
                - Storage of passwords only as hash with salt
                - Regular integrity checking
        - SYS.1.3 Unix server (or similar module)
        - APP.3.1 Web applications
            - The following requirements must also be met in addition to the module requirements:
                - Encrypted transfer of personal data and data for the processing of payment transactions: Business-critical, personal or financial data must be encrypted during transmission in accordance with Directive 4711. The following algorithms and key lengths are permitted [....]
    - [S5] Database server for reserving persisted E-commerce data, including customer data
        - SYS.1.1 General server
            - The following requirements must be met in addition to the module requirements:
                - Regular integrity checking

- In addition, all queries of the customer database must be logged.
- SYS.1.3 Unix server (or similar module)
- APP.4.3 Database
  - The following requirements must be met in addition to the module requirements:
    - Encrypted storage of customer data/payment transaction data

- Payment system
  - [K2] VPN connection to payment transaction service provider
    - NET.3.3 VPN
  - [S1] VPN server
    - SYS.1.1 General server
    - SYS.1.3 Unix server (or similar module)
    - NET.3.3 VPN
  - [S6] Payment server for payment system
    - SYS.1.1 General server
    - SYS.1.3 Unix server (or similar module)
    - NET.3.3 VPN
    - E-payment (see Appendix)
- [C1] IT system for administration and configuration of networks and IT systems
  - SYS.2.1 General client
    - The following requirements must be met in addition to the module requirements:
      - Dual control principle for critical administration activities
  - SYS.2.2.2 Client on Windows 8 (or comparable module)
  - CON.4 Standard software

2.7 Assessment of residual risks/risk handling

When creating IT-Grundschutz profiles, risk analyses usually identify additional security requirements that go beyond the IT-Grundschutz model. These analyses typically also identify risks that cannot all be covered by specified requirements or related safeguards. Such residual risks must be assessed and documented. This documentation should record, among other things, if existing (standard) requirements of a module are not met or if more risks could be covered with additional safeguards.

Furthermore, individual cases may give rise to additional risks which must be dealt with in the context of information security management.

Example: Assessment of residual risks/risk handling

As a rule, only simple password-based procedures are used when authenticating customers. Insofar as the associated risks cannot be borne, stricter procedures (multi-factor authentication) must be applied.

Highly professional targeted attacks cannot be fully pre-emptively mastered according to the current state of the art. Thus the detection of security incidents and the response to them are of particular importance. The relevant risk must be borne.

Distributed denial-of-service attacks have recently increased enormously in terms of impact. High-quality protection against such attacks can only be achieved in cooperation with Internet providers. It is necessary to bear a residual risk that the E-commerce offer may be affected by such attacks.

2.8 Notes on Application

The Notes on Application describe how to deal with the identified requirements within the information security management system (ISMS). They should usually be integrated into the overall safety concept and be subsequently implemented within the company.

Example: Notes on Application

The determined requirements are to be integrated into the overall safety concept and implemented in the course of implementation planning.

2.9 Supporting information

This section provides users with additional information for further research. This information may include references to other IT-Grundschutz modules, other BSI publications, or other sources.

Example: Supporting information

More detailed information on the individual requirements can be found in the implementation information of the individual modules of the IT-Grundschutz.

Specific information on the implementation of the requirements of Section 13 of the German Telemedia Act (TMG) can be found in the BSI publication "Absicherung von Telemediendiensten nach Stand der Technik" (Securing Telemedia Services According to the State of the Art).

2.10 Appendix

When creating an IT-Grundschutz profile, you usually go through almost all of the steps (structural analysis, assessment of protection requirements, modelling, risk analysis) required to create a security concept based on IT-Grundschutz. Further detailed information on these steps may be found in the Appendix.

Under certain circumstances, it may not be possible to fully map the information system or business process considered in the profile with the existing IT-Grundschutz modules. In this case, it is useful to create user-defined modules and include them in the Appendix of the profile. An index of abbreviations or a bibliography or glossary that can be integrated into the Appendix can often prove very useful for users.

Example: Appendix:

- Abbreviations

[...]

- Literature

[...]

- Glossary

[...]

- E-payment module

[...]

- Assessment of protection requirements, risk assessment, etc.

[...]

3 Outlook: Saving time, costs and resources with IT-Grundschutz profiles

The new IT-Grundschutz profiles are to be regarded as practical templates with which different user groups can adapt IT-Grundschutz to their needs. The new IT-Grundschutz profiles can be developed by users in practice, with a clear focus on adaptations that are specific to industries and target groups. The close practical relevance and the model character of the new profiles help organisations of any size to save on effort, time and costs in the individual implementation of IT-Grundschutz.