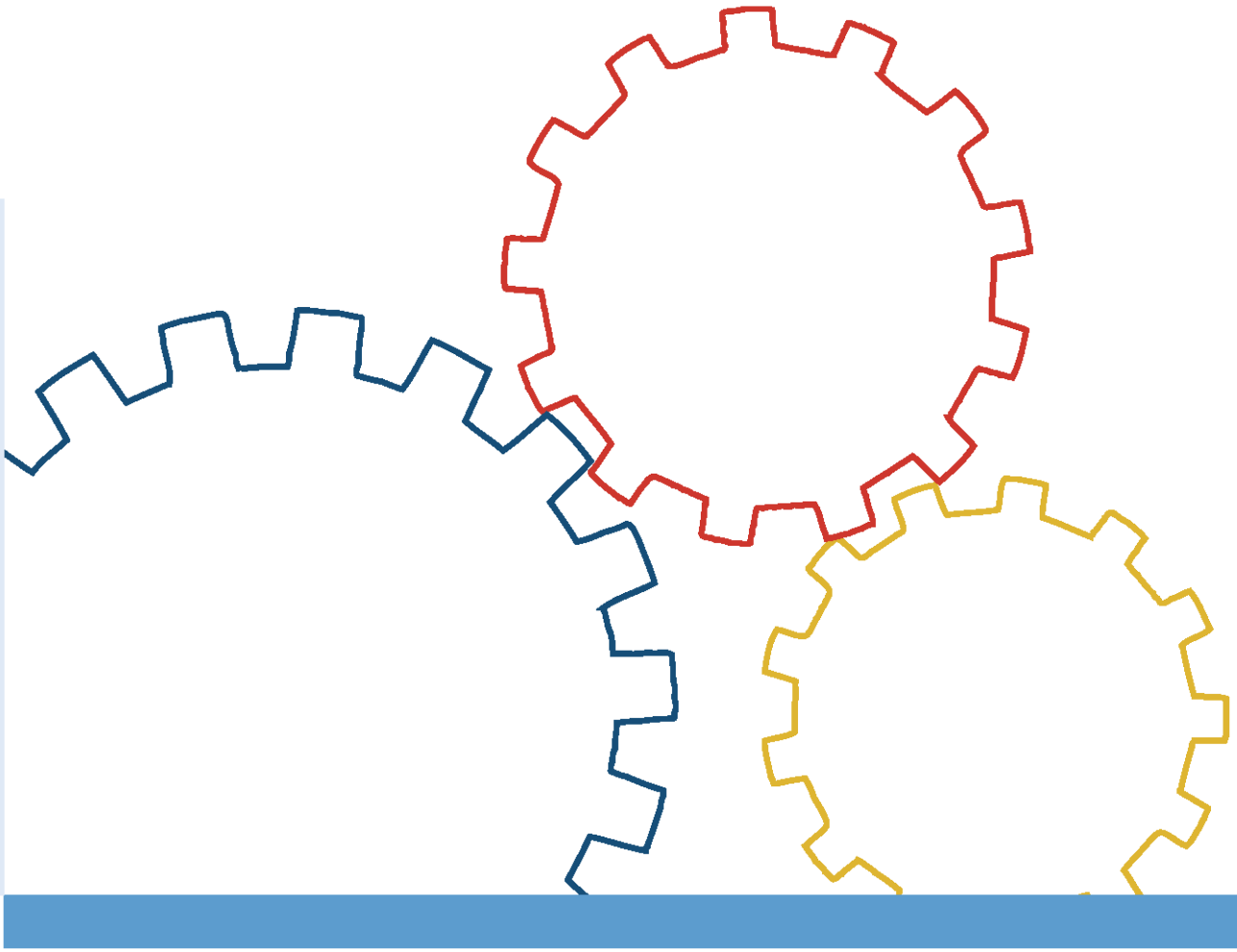
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 200-3

Risk Analysis based on IT-Grundschutz



www.bsi.bund.de/grundschutz

Version 1.0

BSI Standard 200-3:

Risk Analysis based on IT Grundschutz

Version 1.0, October 2017

Federal Office for Information Security (BSI)

Godesberger Allee 185-189, 53175 Bonn

Table of contents

Table of contents

1 Introduction

1 Introduction

1.1 Version history

As per	Version	Changes
October 2016	CD 1.0	Redesigned based on BSI Standard 100-3 • Risk analysis modified on the basis of elementary threats • Matrix approach for evaluating risks introduced • Risk appetite and opportunity management introduced
October 2017	1.0	Incorporation of user comments • Terms "probability of occurrence" and "handling alternatives" replaced by "frequency of occurrence" and "handling options", respectively • Comparison of terms from ISO/IEC 31000 and BSI Standard 200-3 • Section Classification of risks divided into risk assessment and risk evaluation • Scope of the document focused on the representation of the risk analysis • Glossary revised

1.2 Objective

With the BSI Standard 200-3 the BSI provides an easy to apply and recognized procedure which allows organisations the adequate and targeted control of their information security risks. The procedure is based on the elementary threats described in the IT-Grundschutz Compendium on the basis of which also the IT-Grundschutz-modules were drawn up.

When the methodology according to IT-Grundschutz is used, a risk evaluation is performed implicitly for areas with normal protection requirements by the BSI when drawing up the IT-Grundschutz modules. Only those threats which have such a high frequency of occurrence or such drastic consequences that security safeguards must be taken are considered. Typical threats that everyone must protect themselves against include, for example, damage due to fire, water, burglary, malware or hardware defects. This approach has the advantage that IT-Grundschutz users do not have to carry out an individual threat and vulnerability analysis for a major part of the information system, since this assessment has already been performed in advance by the BSI.

In certain cases, however, an explicit risk analysis must be carried out, for example if the information system considered includes target objects which

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

In these cases, the following questions arise:

- Which threats for the information are not adequately allowed for, or are not even factored in at all, in the implementation of the IT-Grundschutz modules?
- Might it be necessary to schedule and implement supplemental security safeguards over and above the IT-Grundschutz model?

This document outlines how it can be determined for specific target objects whether and in what respect there is any need to take action over and above the IT-Grundschutz in order to reduce risks for information processing. For this, the risks emanating from elementary threats are estimated and assessed using a matrix. The assessment is carried out using the frequency of occurrence and the extent of damage resulting when the damage occurred. The respective risk is derived from these two parameters.

In this BSI Standard 200-3, the risk analysis consists of two steps. In a first step, the threat summary compiled in Section 4 is worked off systematically. For every target object and every threat, an evaluation is performed assuming that security safeguards have already been implemented or planned (see examples in Section 5). These are usually the security safeguards which have been derived from the basic and standard requirements of the IT-Grundschutz Compendium. The first evaluation is followed by another evaluation in which security safeguards for risk treatment are considered (see examples in Section 6). By means of a before-and-after comparison, the effectiveness of the security safeguards which were used to treat risks can be checked.

1.3 Differentiation, terms and classification within the IT-Grundschutz

Opportunities and risks are the predictions frequently based on calculations of a possible benefit in the positive case or damage in the negative case. The definition of advantage or damage depends on the benchmark values of an organisation.

This standard focuses on considering the negative effects of risks, aiming at showing adequate safeguards for minimising risks. In practice, only the negative effects are considered as part of the management in most cases. Additionally, organisations should nevertheless also look at the positive effects.

Risk analysis

In this standard, the term “risk analysis” refers to the complete process for determining (identifying, assessing and evaluating) and treating risks. However, according to the relevant ISO standards ISO 31000 (see [31000]) and ISO 27005 (see [27005]), “risk analysis” only refers to a single step as part of the risk determination, which consists of the following steps:

- Risk Identification
- Risk Analysis
- Risk Evaluation

In the meantime, however, the term “risk analysis” has been established for the entire process of risk determination and risk treatment. Therefore, the term “risk analysis” is still used in the IT-Grundschutz and also this document to refer to the comprehensive process.

The risk analysis according to BSI Standard 200-3 provides for the following steps (see also Figure 1), which are considered in greater detail in the relevant sections.

- Step 1: Drawing up of a threat overview (see Section 4)
    - Compiling of a list of potential elementary threats
    - Determination of additional threats, which go beyond the elementary threats and arise from the specific operational scenarios
- Step 2: Risk classification (see Section 5)

  - Risk assessment (determination of frequency of occurrence and extent of damage)
  - Risk evaluation (determination of the risk category)
- Step 3: Risk treatment (see Section 6)
  - Risk avoidance
  - Risk reduction (determination of security safeguards)
  - Risk transfer
  - Risk acceptance
- Step 4: Consolidating of the security concept (see Section 7)
  - Integration of the additional safeguards identified based on the risk analysis in the security concept

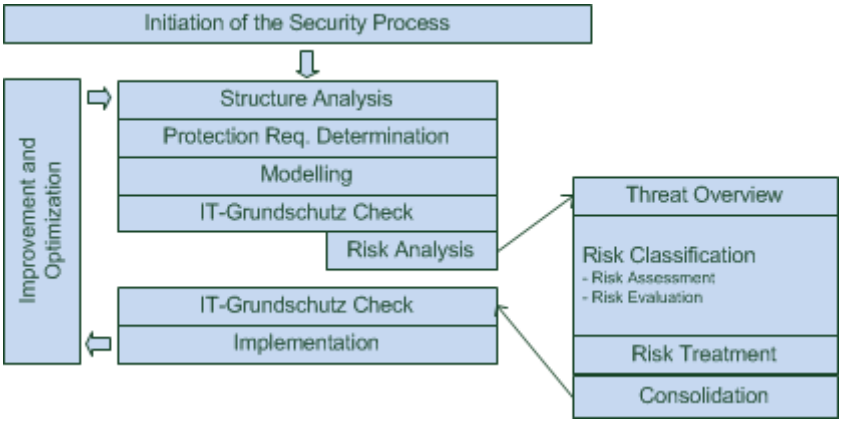


Figure 1: Integration of the risk analysis into the security process

In the international standards, in particular in ISO 31000, some terms are used with a different meaning than in this standard. Therefore, a table can be found in the Appendix, which compares the most important terms of ISO 31000 and the 200-3 (see Table 10).

1.4 Addressees

This document is aimed at those who are responsible for security, experts, consultants and everyone who is in charge of managing or carrying out risk analyses for information security.

This standard can be used when companies or public agencies are already working successfully with IT-Grundschutz Methodology according to BSI Standard 2002-2 (see [BSI2]) and would like to add a risk analysis directly to the IT-Grundschutz. However, depending on the framework conditions of an organisation and the type of information system, it may be appropriate to use a different established practice or an adapted methodology for the analysis of information risks as an alternative to the BSI Standard 200-3.

1.5 Application

This document describes a methodology to analyse risks. It can be used to supplement an IT-Grundschutz security concept. The list of elementary threats contained in the IT-Grundschutz Compendium is used as an aid. It is recommended to apply the methodology described in Sections 2 through 8 step by step.

In the BSI Standard 100-4 *Business Continuity Management* (see [BSI4]), a risk analysis which differs from the risk analysis described in this document only in some terms is also provided for particularly critical resources of the business processes of the organisation. Both risk analyses can be adapted to each other efficiently. It makes sense that all roles in an organisation dealing with risk

management for a specific area coordinate things with each other and choose comparable methodologies and approaches.

2 Preliminary work for the risk analysis

Before starting the actual risk analysis, the following preliminary work should have been completed as specified in the IT-Grundschutz Methodology according to BSI Standard 200-2:

- A systematic information security process should have been initiated. This process is used to work off the activities in the field of information security in a structured manner. For example, appropriate roles and tasks must be defined.
- According to Section 3.3 of the IT-Grundschutz Methodology, a scope must have been defined for the security concept. This scope is referred to below as the information system.
- A structure analysis should have been performed for the information system according to Section 7.4 or 8.1 of the IT-Grundschutz Methodology. This is a way of ascertaining the key information about the information system, for example business processes, the network plan and a list of the most important applications which depend on the IT systems.
- Subsequently, an assessment of protection requirements should have been performed according to Section 7.5 or 8.2 of the IT-Grundschutz Methodology. The result is the protection requirements of the business processes, applications, IT systems, rooms used as well as a list of the critical communication connections. The protection requirements refer to the core values of confidentiality, integrity and availability and is usually determined at the levels “Normal”, “High” and “Very high” according to IT-Grundschutz.
- A modelling process should have been performed, as specified in Section 7.6, 8.3 of the IT-Grundschutz Methodology and Section 2 of the IT-Grundschutz Compendium. It is determined for each target object in the information system whether there are corresponding IT-Grundschutz modules and how they are to be applied. The security requirements stated in the individual modules and the security safeguards derived from them form the basis for the IT-Grundschutz security concept of the information system under review.
- Prior to the risk analysis, an IT-Grundschutz check according to Section 7.7 or 8.4 of the IT-Grundschutz Methodology should be performed. This determines which basic and standard security requirements have already been met for the information system under review and where there are still deficits.

The result of this preliminary work is a list of the target objects for which a risk analysis should be carried out ("target objects under review"). To ensure that this task can be performed with reasonable effort, it is important that the target objects have reasonably been summarised in groups according to IT-Grundschutz Methodology.

If many target objects have to be subjected to a risk analysis despite the formation of groups, they should be prioritised appropriately:

- If the "standard protection" methodology was chosen for IT-Grundschutz, priority should be given to the processing of higher-level target objects (especially business processes, subsystems and entire information system). This work often leads to valuable reference points for the risk analyses of the lower-level technical target objects.
- If the "core protection" methodology was chosen for IT-Grundschutz, priority should be given to the processing of the target objects with the highest protection requirements.
- If the "basic protection" methodology was chosen for IT-Grundschutz, risk analyses are not performed initially, but only the basic requirements are implemented first.

It is possible to deviate from the methodology described in this document. Under certain circumstances, it is a good idea to perform a risk analysis only after the IT-Grundschutz requirements

have been met. This can for example make sense for target objects which are already in use and can be described adequately by IT-Grundschutz modules. As an aid to making a decision after which step a risk analysis makes sense, a compilation of the advantages and disadvantages of the possible points in time can be found in Section 8.5 of the IT-Grundschutz Methodology (see [BSI2]).

Note: The target objects examined do not necessarily have to be system-oriented target objects (e.g. applications, IT systems or rooms). The risk analysis can rather also be performed on a business process level.

The preliminary work also includes that the basic prerequisites for the risk analysis are specified by the organisation's management. To this end, the management level must adopt a policy for handling risks. It should cover the following aspects, amongst other things:

- Under which prerequisites does a risk analysis have to be carried out in any case?
- Which methodology and/or which standard is used to identify, assess, evaluate and treat the risks?
- How is the methodology chosen adjusted to the particular interests of the organisation?
- What are the risk acceptance criteria?
- Which organisational units are responsible for which subtasks of the risk analysis? Are risks assigned to the relevant risk owners?
- How are risk analyses integrated into the security process, for example prior to or after the implementation of the IT-Grundschutz requirements?
- Which obligations to report exist within the scope of risk analyses?
- At what intervals does the risk analysis have to completely updated?

Since the risk acceptance criteria of an organisation greatly depend on its risk appetite, it can make sense to also describe the risk appetite (see Section 9) in the policy. An organisation might not be aware of its own risk appetite or has only a vague idea of this term. In this case, the management level should bring about clarification and decisions and, if necessary, the organisation should involve experts from outside.

The management level's specifications described in the risk analysis policy must be implemented consequently when risks are evaluated and treated. Cases of doubt may arise for example if it does not make sense to apply the risk appetite defined for a certain risk. Those exceptional cases should be coordinated and documented.

The risk analysis policy should be drawn up according to the specifications of the information security management system (see BSI Standard 200-2 *IT-Grundschutz Methodology* [BSI2]). It must be checked at regular intervals or due to special events whether it is still up to date and, if necessary, adapted based on the organisation's objectives. In particular, the methodology used for the risk analysis should also be checked at regular intervals. The risk analysis policy must be approved by the organisation's management.

Example 1:

Using a fictional organisation, RECPLAST GmbH, as an example, the following shows how risks can be assessed, evaluated and treated. It should be noted that the structure of RECPLAST GmbH is by no means optimal as regards information security. The example is simply used to illustrate the procedure of performing risk analyses.

RECPLAST GmbH is a fictional organisation with around 500 employees, 130 of whom have their own workstations. RECPLAST GmbH is distributed over two sites within the city of Bonn, where, among others, the administrative and producing tasks are performed, and three distribution sites in Germany.

The IT network is divided into several subnetworks. For the examples in this risk analysis, the Subnetwork A (see Figure 2 in Section 4) is examined in more detail. Access to the Subnetwork A is secured by means of the Firewall N1. The servers S1 (Virtualisation Server) and S5 are connected by means of individual switches.

The Virtualisation Server S1 provides several service. For example file and email servers are operated in virtual machines on this server. The applications partially have high protection requirements in at least one of the three core values of confidentiality, integrity or availability. Due to the maximum principle, the highest protection requirements of the virtual machines and/or IT applications made available apply to the Virtualisation Server S1. To record the hours worked of the employees, RECPLAST GmbH uses a software solution which is implemented as a web application. For storing data, it uses a database which is operated in the Database Management System (A1) on Server S5.

Moreover, RECPLAST GmbH operates a series of servers which are used to continuously monitor all IT systems and the applications operated on them.

Example 2:

The fictional company MUSTERENERGIE GmbH operates a smart meter gateway infrastructure (intelligent network). Central components of such an infrastructure are intelligent measurement systems, also referred to as "smart metering systems". The Smart Meter Gateway (SMGW) is the central communication unit. It communicates in the local area with the end customer’s electronic meters (Local Metrological Network, LMN area), with devices from the Home Area Network (HAN area) and with authorised market participants in the Wide Area Network (WAN area). Moreover, the SMGW makes it possible that local devices of the HAN connect to authorised market participants via the WAN.

The Smart Meter Gateway Administrator (SMGW Admin) is responsible for the installation, commissioning, operation, maintenance and configuration of the SMGW. As it is sometimes sensitive information, the protection of this information is important. It must therefore be ensured that the IT is securely operated by the SMGW Admin.

For the examples in this risk analysis, the Smart Meter Gateway Administration of MUSTERENERGIE GmbH is also examined in more detail in addition to the Subnetwork A of RECPLAST GmbH.

3 Summary of the elementary threats

From the large number of specific individual threats of the IT-Grundschutz modules, the BSI has identified the general aspects and transferred them in 47 elementary threats which are listed in the IT-Grundschutz Compendium. When drawing up the overview of the elementary threats, the objectives described below were pursued. Elementary threats are

- Optimised for use in the risk analysis
- Product-neutral (always), technology-neutral (if possible, certain techniques influence the market to such an extent that they also influence the abstracted threats)
- Compatible with comparable international catalogues and standards and
- Seamlessly integrated into IT-Grundschutz.

Since the elementary threats are mainly intended to make it possible to efficiently perform risk analyses, it was focused on naming real threats. Threats which mainly address the lack of or inadequate implementation of security safeguards and thus refer to indirect threats were deliberately not specified. When drawing up the overview of the elementary threats, it was also considered which core value of information security (confidentiality, integrity, availability) would be damaged by the respective threat. As this information is of interest for different steps of the security concept, it is also listed in the table below. Not all elementary threats can be mapped to precisely one core value, and equally different threats affect several core values. This must be interpreted in such a way that the listed core values are directly impaired by the respective threat. For many threats, it can be discussed to what extent all three core values could be affected, because also indirect effects can be derived. For G 0.1 *Fire*, for example, “availability” is mentioned as the only core value affected. Of course, a fire could also damage a data medium in such a way that the information stored is still available, but its integrity is impaired. Another scenario could be that confidential documents could be accessed by unauthorised persons due to rescue measures in the case of a fire. This would be indirect effects on the core values of confidentiality and integrity, but only the availability is directly impaired.

The table below contains the overview of the elementary threats as well as the specification of the mainly affected core values. C for stands for confidentiality, I for integrity and A for availability.

	Threat	Core value
G 0.1	Fire	A
G 0.2	Unfavourable environmental conditions	I,A
G 0.3	Water	I,A
G 0.4	Soiling, dust, corrosion	I,A
G 0.5	Natural catastrophes	A
G 0.6	Catastrophes in the environment	A
G 0.7	Major events in the environment	C,I,A
G 0.8	Disruption or malfunction of power supply	I,A
G 0.9	Failure or malfunction of communication networks	I,A
G 0.10	Failure or malfunction of supply networks	A
G 0.11	Failure or malfunction of service providers	C,I,A
G 0.12	Electromagnetic interference	I,A
G 0.13	Interception of compromising radiation	C
G 0.14	Espionage	C
G 0.15	Line tapping	C
G 0.16	Theft of devices, data media and documents	C,A
G 0.17	Loss of devices, data media and documents	C,A
G 0.18	Poor planning or lack of adjustment	C,I,A
G 0.19	Disclosure of information that should be protected	C
G 0.20	Information from unreliable sources	C,I,A
G 0.21	Manipulation of hardware or software	C,I,A
G 0.22	Manipulation of information	I
G 0.23	Unauthorised entry into IT systems	C,I
G 0.24	Destruction of devices or data media	A
G 0.25	Failure of devices or systems	A
G 0.26	Malfunctions of devices or systems	C,I,A
G 0.27	Lack of resources	A
G 0.28	Software vulnerabilities or errors	C,I,A
G 0.29	Violation of laws or contracts	C,I,A
G 0.30	Unauthorised use or administration of devices and systems	C,I,A
G 0.31	Incorrect use or administration of devices and systems	C,I,A
G 0.32	Misuse of authorisations	C,I,A
G 0.33	Loss of personnel	A
G 0.34	Attack	C,I,A
G 0.35	Coercion, extortion or corruption	C,I,A
G 0.36	Identity theft	C,I,A
G 0.37	Repudiation of acts	C,I
G 0.38	Misuse of personal data	C
G 0.39	Malware	C,I,A
G 0.40	Denial of services	A
G 0.41	Sabotage	A
G 0.42	Social engineering	C,I
G 0.43	Importing messages	C,I
G 0.44	Unauthorised entry into rooms	C,I,A
G 0.45	Loss of data	A
G 0.46	Loss of integrity of information that should be protected	I
G 0.47	Harmful side effects	C, I, A

Table 1: Overview of the elementary threats with the relevant affected core values

4 Drawing up of a threat overview

The aim of the following work steps is to produce, as a starting point for the risk analysis, a summary of the threats to which the information system's target objects under review are subject. The result of this preliminary work (see Section 2) is a list of (prioritised) target objects for which a risk analysis should be carried out. It is used as a basis for preparing the threat summary. This list is supplemented by the higher-level target object "information system" unless this target object is already included in the list anyway. When determining threats, the BSI uses a two-stage approach. The relevant elementary threats are identified first and, based on them, other possible threats (additional threats) going beyond the elementary threats are determined.

4.1 Determination of elementary threats

Which approach is used to determine elementary threats depends on whether the target object under review can be mapped adequately with existing modules of the IT-Grundschutz Compendium or not. For existing modules, a risk analysis has already been carried out in advance and the relevant elementary threats have therefore already been determined for them and can be used as a starting point of the threat analysis. For each target object, the number and title of these threats are collected and assigned to the respective target object. Moreover, the list of elementary threats is used and it is checked whether other elementary threats are relevant to the target object, i.e. can *in principle* lead to *substantial damage*. Any additional elementary threat must then be evaluated as to whether it can directly, indirectly or not at all impact on the target object:

- "Directly relevant" means in this case that the respective threat can impact on the target object under review and thus has to be treated as part of the risk analysis.
- "Indirectly relevant" means in this case that the respective threat can impact on the target object under review, but does not go beyond other (more general) threats in its potential effect. In this case, the respective threat for this target object does not have to be treated separately as part of the risk analysis.
- "Not relevant" means in this case that the respective threat cannot impact on the target object under review and thus does not have to be treated for this target object as part of the risk analysis.

Threats which are only "indirectly relevant" or "not relevant" to a certain target object, however, can of course be "directly relevant" to other target objects in the same information system.

In practice, the type of the respective target object has a major impact on which elementary threats can be applied to it at all. The threat G 0.28 *Software vulnerabilities or errors*, for example, will only rarely be relevant to one office room, but rather to the clients operated in it. Threats which do not relate to specific technical components, for example G 0.29 *Violation of laws or regulations*, are in most cases suitable for target objects of the type application, business process or entire information system.

Example:

If a specific server operating system is examined, the elementary threat G 0.25 *Failure of devices or systems* is for example a relevant threat against which specific security safeguards must be taken under certain circumstances. The elementary threat G 0.1 *Fire*, however, is irrelevant to a specific server operating system. An operating system does not offer specific safeguards against fire. Considering G 0.1 *Fire* would not result in new aspects with regard to G 0.25 *Failure of devices or systems*.

Threat	Core values	Impact and relevance	Comment
G 0.1 Fire	Availability	Indirect impact/not relevant	The threat for an operating system caused by fire is irrelevant. Considering G 0.1 *Fire* would not cover new aspects with regard to G 0.25 *Failure of devices or systems*.
G 0.9 Failure or malfunction of communication networks	Availability, integrity	Indirect impact/not relevant	The threat for an operating system caused by *Failure or malfunction of communication networks* is indirect. Considering G 0.9 would not result in new aspects with regard to G 0.26 *Malfunctions of devices or systems*. An operating system does not offer specific safeguards against G 0.9, which means that the threat is not relevant in this case. No specific safeguards are required.
G 0.25 Failure of devices or systems	Availability	Direct impact/ relevant	The threat caused by G 0.25 *Failure of devices or systems* directly impacts on an operating system. For this reason, safeguards against G 0.25 *Failure of devices and systems* must be checked.
G 0.26 Malfunctions of devices or systems	Confidentiality, availability, integrity.	Direct impact/ relevant	The threat caused by G 0.26 *Malfunctions of devices or systems* directly impacts on an operating system. For this reason, safeguards against G 0.26 *Malfunctions of devices and systems* must be checked.

Table 2: Example of determining elementary threats for a server operating system

If the target object under review cannot be mapped adequately with existing modules of the IT-Grundschutz Compendium, as topics are concerned which are not or not adequately covered in the IT-Grundschutz Compendium so far to be able to model the information system under review, the list of the 47 elementary threats is used and it is checked for each target object which threats are relevant. The same methodology as described above can be applied.

The result of the previous steps is a table that assigns a list of relevant elementary threats to each target object. In order to facilitate the subsequent analysis, the protection requirement for each target object that was determined for the three basic parameters of confidentiality, integrity and availability when determining the protection requirement should be listed in the table. This assignment is not required for the higher-level target object *information system.*

Below, it is shown using two examples how the threat summary can be prepared based on elementary threats.

Example 1:

At its site in Bad Godesberg, RECPLAST GmbH operates a centrally administrated network with 130 connected workstations. The workstation computers are equipped with common office applications (standard software for word processing, spreadsheet and presentation programs) and client software for email and Internet usage. In addition to this, special software is installed on different workstation computers depending on the area of responsibility.

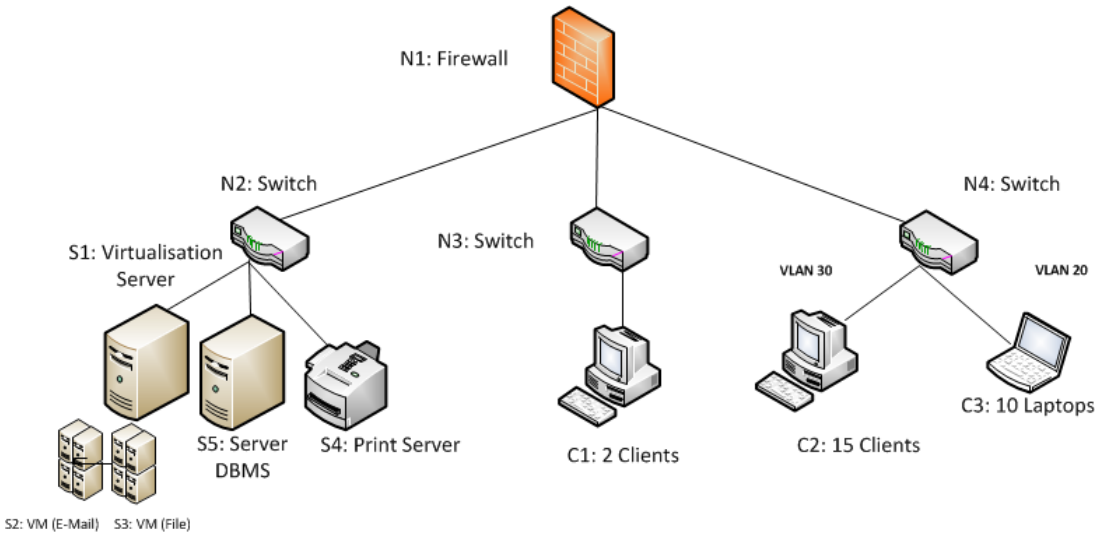


Figure 2: Excerpt of a network plan (RECPLAST Subnetwork A)

As part of the assessment of protection requirements, high and/or very high protection requirements have been determined for the following target objects (see Table 3) in at least one of the three core values (confidentiality, integrity or availability). They must therefore be subjected to a risk analysis.

- Firewall N1
- Switches N2, N3 and N4,
- Virtualisation Server S1, Virtual Machines S2 and S3, DBMS Server (S5) and Database Management System A1 (Database A1 for short),
- Laptops C3 and Clients C1

(Excerpt RECPLAST GmbH Subnetwork A)

Number	Title of module	Target object
ISMS.1, ORP.1 etc.	*Security management, organisation etc.*	IV
INF.5	*Computer centre*	M.1, M.2
INF.8	*Office workplace*	M.3
NET.3.2	*Firewall*	N1
NET.3.1	*Routers/switches*	N2, N4
NET.3.1	*Routers/switches*	N3
SYS.1.5	*Server virtualisation*	S1
APP.5.1	*Email/groupware*	S2 (VM1)
APP.3.3	*File server*	S3 (VM2)
SYS.1.2.2	*Windows Server 2012*	S5
APP.4.3	*Relational database systems*	A1
SYS.2.2	*Windows clients*	C1
SYS.2.3	*Clients under Unix (laptops)*	C3

Table 3: List of the target objects under review (excerpt)

Example 2:

When modelling the information system on which the Smart Meter Gateway Administration is based, it has been determined that no IT-Grundschutz module can be assigned to the target object “Smart Meter Gateway Administration Zx”. It must therefore also be subjected to a risk analysis.

(Excerpt Smart Meter Gateway Administration)

Number	Title of module	Target object
-	-	Smart Meter Gateway Administration Zx

Table 4: List of the target objects under review (excerpt)

The tables below provide an overview of relevant elementary threats for the target objects under review (Virtualisation Server S1, Database A1) and Smart Meter Gateway Administration Zx. They serve as the starting point for the subsequent *determination of additional threats*.

Virtualisation Server S1
Confidentiality: High Integrity: High Availability: High
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*

Table 5: Threat summary for the target object S1 (excerpt)

Database A1

Database A1
Confidentiality: High Integrity: High Availability: High
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 0.20 *Information from unreliable sources* G 0.21 *Manipulation of hardware and 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 0.27 *Lack of resources* 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 0.37 *Repudiation of acts* G 0.39 *Malicious software* 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*

Table 6: Threat summary for the target object A1 (excerpt)

Smart Meter Gateway Administration Zx
Confidentiality: High Integrity: High Availability: High
G 0.18 Poor planning or lack of adjustment *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 0.43 Importing messages* *etc.*

Table 7: Threat summary for the target object Zx (excerpt)

4.2 Determination of additional threats

For the target objects under review, there might be individual additional threats under certain circumstances, which go beyond the elementary threats and arise from the specific operational scenario or individual application. These must also be taken into consideration.

For information security, the *relevant threats* are those

- That could produce substantial damage
- Are realistic for the current application and area of use

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.

Note: If an organisation identifies another *generic* threat as part of this step, which is so far not included in the IT-Grundschutz Compendium, it should inform the BSI about this to ensure that the catalogue of the elementary threats can be extended accordingly.

When determining additional relevant threats, the protection requirements of the respective target object under review should be considered in terms of the three *core values* of information security, i.e. *confidentiality*, *integrity* and *availability*:

- If a target object has a *very high* protection requirement for a particular core value, the threats that could adversely affect this basic parameter should be found first.
- Even if a target object has *high* protection requirements for a particular core value, the threats that could adversely affect this core value should be found.
- If the target object has *normal* protection requirements in a certain core value, the recommended security requirements are usually sufficient for this core value if the target object can be modelled with the existing IT-Grundschutz modules.

Irrespective of the protection requirements of the target object under review, it is particularly important to identify any additional relevant threats if there is no appropriate module for the target object in the IT-Grundschutz Compendium or if the target object is operated in a scenario (environment, application) which is not foreseen in the IT-Grundschutz Compendium.

Information as which questions are to be taken into consideration when identifying additional threats can be found in the Appendix (see Section 9).

It is frequently the case that in practice additional threats affect several target objects. The identified additional threats are added to the threat summary.

Important: If relevant threats are not considered, this may produce gaps in the resulting security concept. If in doubt a careful analysis of whether and (if so) which threats may still be missing should therefore be performed. For this, it is often advisable to rely on external consulting services.

In practice, brainstorming involving all employees involved has proven effective in identifying additional threats. Information security officers, specialists responsible, administrators and users of the target object under review as well as external experts, if appropriate, should be involved. The participants' objectives should be clearly formulated and the brainstorming time limited. An information security expert should moderate the brainstorming.

Example (excerpt RECPLAST)

In the scope of a brainstorming session, the company RECPLAST identifies such additional threats as the following:

Entire information system
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 specifies the elementary threats G 0.21 *Manipulation of hardware or software* and G 0.22 *Manipulation of information*.
etc.

Switch N3
Confidentiality: Normal Integrity: Normal Availability: High
T z.2 *Damage to information technology in production department*
The Client C1 and Switch N3 are operated in the company's production department and are therefore subject to particular, physical threats. The devices can be damaged, destroyed or their lifespan reduced. (Specification of G 0.24 *Destruction of devices or data media*)
etc.

Database A1
Confidentiality: High Integrity: High Availability: High
As part of the brainstorming, no additional threats were identified, but it was determined that additional security requirements are required to reduce the threats G 0.28 *Software vulnerabilities or errors* and G 0.32 *Misuse of authorisations* in the case of high protection requirements. This result is earmarked for the work step “Treatment of risks”.

5 Classification of risks

5.1 Risk assessment

After all relevant threats have been identified (see Section 4), the risk arising from a threat is determined in the next step. How high this risk depends both on the frequency of occurrence (occurrence assessment) of the threat and on the extent of the imminent damage. When assessing risks, both influencing factors must therefore be taken into account.

In order to assess risks with reasonable effort, there is no simple universal concept. The risk element *extent of damage* can only be assessed by the organisation itself. Here, the spotlight is on how the occurrence of a threat can have an impact, i.e. which financial or other damage, which direct damage and which consequential damage can occur. It also considers whether, with what effort and in what time the damage is to be repaired.

The *frequency of occurrence* must be assessed by suitable qualified staff and can be supported by statistics and own experiences. With respect to statistics, however, it must be taken into account under which framework conditions they were created, since statistics, too, have been compiled for a special purpose and cannot be transferred automatically to the special interests of the organisation. Moreover, the interpretation of statistic results generally involves uncertainties.

As a matter of principle, risks can be considered either qualitatively or quantitatively. The quantitative risk assessment is very complex and requires comprehensive statistical data. In most cases, such comprehensive empirical values are missing in the very dynamic environment of information security. In most cases, it is therefore more practical to work with qualitative categories for both the frequency of occurrence and the potential extent of damage. Per dimension, not more than five categories should be chosen.

In order to assess risks, IT-Grundschutz uses the categories described below. Every organisation can individually define both number of steps and the criteria. It should use categorisations which fit best its management system.

- Frequency of occurrence: Rarely, Medium, Frequently, Very frequently
- Potential extent of damage: Negligible, Limited, Considerable, Threatening the existence of the organisation

Note: Every organisation should coordinate the descriptions of the categories in particular with the specialised departments so that all employees can easily understand their meaning. If a specific risk is assessed by two different employees of an organisation, the same result should be obtained.

Frequency of occurrence/description	
Rarely	According to present knowledge, the event could occur every 5 years at the most.
Medium	The event occurs once every 5 years to once a year.
Frequently	The event occurs once a year to once a month.
Very frequently	The event occurs several times a month.

Table 8: Categorisation of frequencies of occurrence

Extent of damage/effects 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 can reach a catastrophic level that threatens the existence of the organisation.

Table 9: Categorisation of the effects of damage

There are organisations working with more differentiated categories in order to meet the needs in different departments or business processes. In practice, however, often only few categories are used per dimension. The majority of users even tends to de facto work with only two categories per dimension, for example "Limited" and "Considerable".

5.2 Risk evaluation

On the basis of the previously defined categories for the potential extent of damage as well as the classification for the frequencies of occurrence of threats, the BSI defines the following risk matrix (see Figure 3). It is simply used to illustrate the following examples and should be adapted to the individual needs

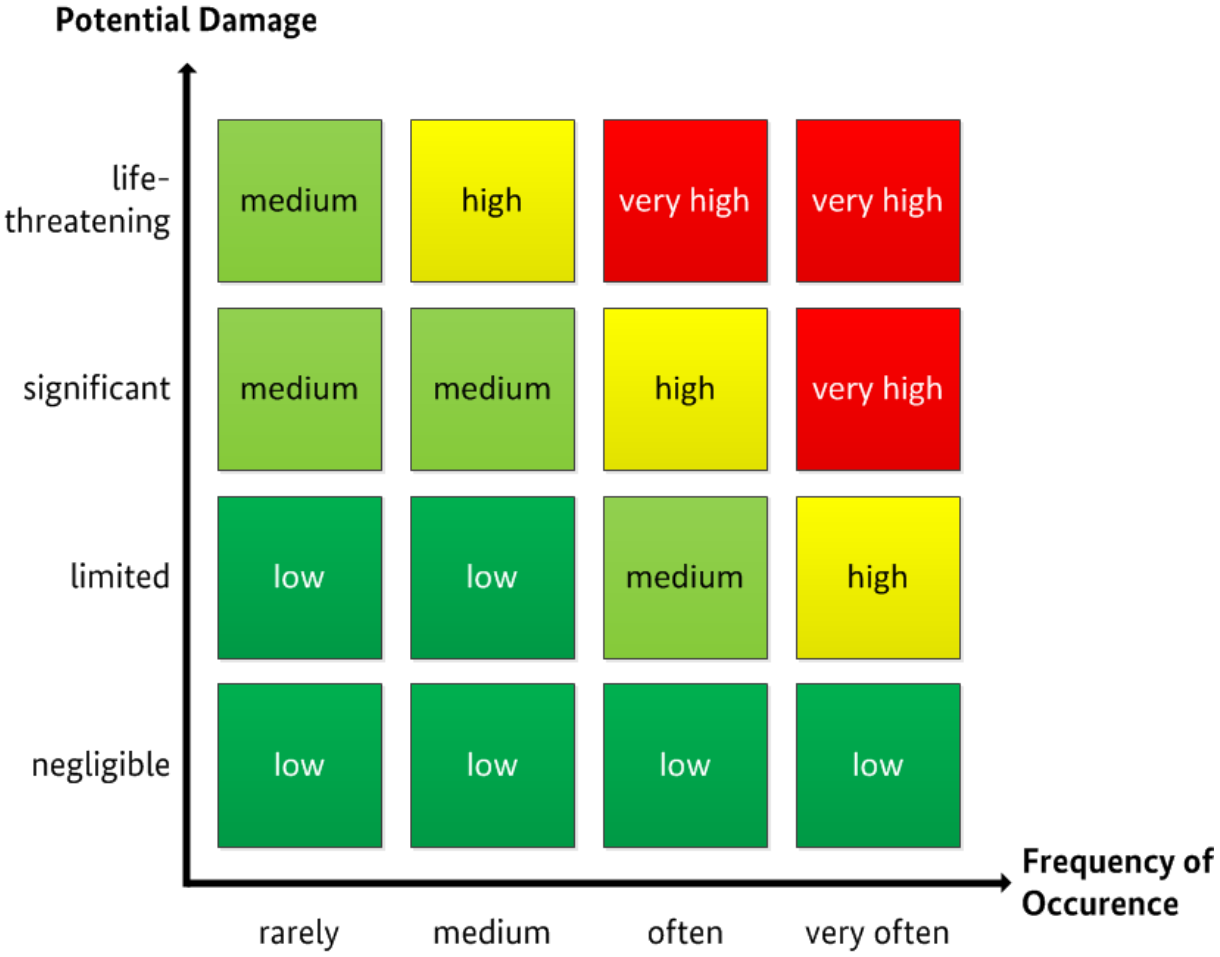


Figure 3: Matrix to classify risks

Risk categories	
Low	The security safeguards already implemented or at least envisaged in the security concept provide adequate protection. In practice, it is common to accept low risks and to still monitor the threat.

Medium	The security safeguards already implemented or at least envisaged in the security concept might not be sufficient.
High	The security safeguards already implemented or at least envisaged in the security concept do not provide adequate protection against the respective threat.
Very high	The security safeguards already implemented or at least envisaged in the security concept do not provide adequate protection against the respective threat. In practice, very high risks are rarely accepted.

Table 10: Definition of risk categories

After risks have been identified, assessed and evaluated, the further procedure (risk treatment strategy) differs greatly from organisation to organisation. The BSI cannot give a general recommendation for selecting a particular treatment strategy, because many individual aspects have to be taken into account. In particular, the risk treatment strategy greatly depends on the risk appetite of the respective organisation(see Section 9).

Note: It is frequently the case that when classifying risks, initial ideas are found for security safeguards that counteract the threats. These suggestions are useful for the subsequent work steps and should be recorded.

The classification of risks provides an overview of the extent of the risks resulting from the threats for the respective target object. The security safeguards planned or already implemented are taken into consideration. Treating these threats is discussed in the next section.

Example (excerpt):

For RECPLAST GmbH, a classification of risks for

- the Virtualisation Server S1 (for the threats G 0.15 *Line tapping* and G 0.25 *Failure of devices or systems*) as well as
- the Database Management System A1 (for the threats G 0.*28 Software vulnerabilities or errors* and G 0.32 *Misuse of authorisations*)

was performed on the basis of the threat summary. The result can be obtained from the following tables.

Virtualisation Server S1 Confidentiality: High Integrity: High Availability: High		
Threat G 0.15 *Line tapping (here: live migration)*	Core values impaired: Confidentiality	
Frequency of occurrence without additional safeguards: Rarely	Effects without additional safeguards: Considerable	Risk without additional safeguards: Medium
Description: To be able to maintain the Virtualisation Server S1, all virtual machines (VMs) run on it are moved to the Virtualisation Server S6 (live migration). The current memory content of the VMs is transferred from S1 to S6. For performance reasons, encrypting the information is abstained from so that the data flow can generally be read. The data flow from Virtualisation Server S1 to the connected central storage systems is also unencrypted. Thus, it is possible to record confidential information. **Evaluation:** To be able to operate the virtual infrastructure securely, suitable segmentation has been taken into		

account on the network level. The individual network segments (e.g. management network, network for live migration or storage network) are separated from each other and configured in such a way that they cannot be accessed from outside. Only authorised administrators are allowed to access the live-migration network. The administration of the virtual infrastructure is integrated into the central rights management of the information system.

Since only authorised administrators are allowed to access the live-migration network, the memory content of the VMs transmitted can only be read by them. However, the administrators are trusted so that the probability for tapping is assessed as "Rarely". The effects, however, are evaluated as "Considerable" due to the confidentiality of the contents transmitted, resulting in a medium risk.

Database A1 Confidentiality: High Integrity: High Availability: High		
Threat G 0.28 *Software vulnerabilities or errors*		Core values impaired: Confidentiality, integrity, availability
Frequency of occurrence without additional safeguards: Frequently	Effects without additional safeguards: Considerable	Risk without additional safeguards: High

Description:

To record the working hours of the employees, RECPLAST GmbH uses a software solution which is implemented as a web application. All employees can access the web application and independently enter their hours worked. The entered hours worked are checked and approved by the heads of departments. In addition to this, the payrolls are made available to the employees via the web application at the end of the month. For storing data, the application uses a database which is operated in the database management system (DBMS).

In the version, the web application contains a known SQL injection vulnerability which can be exploited relatively easily. For the web application, updates are no longer available, as the manufacturer of the software solution has gone bankrupt.

Evaluation:

On the database management system, all authorisations must be granted as restrictively as possible in order to prevent that the security gap of one application has effects on the databases of other applications. The effects of the SQL injection vulnerability of the web application thus remain restricted to the data of the web application itself.

Since the SQL injection vulnerability of the web application is publicly known and can be exploited relatively easily, the probability is assessed to be "Frequently". If the gap is exploited successfully, this will affect the confidentiality and integrity of the entered hours worked, the approval of the hours worked and the payrolls. The effects are therefore assessed as "Considerable". This results in a high risk.

Note: Since often a very large number of target objects and a very large number of threats have to be dealt with, the continuous text is optional for the description and evaluation of a threat and only used in the examples above to comprehensibly represent the result of the evaluation. The safeguards mentioned in the table are usually safeguards derived from the basic and standard requirements of the IT-Grundschutz Compendium. The following presentation (evaluation of the threats G 0.25 *Failure of devices or systems*, G 0.32 *Misuse of authorisations* etc.) is fully sufficient for risk evaluations.

Virtualisation Server S1 Confidentiality: High Integrity: High Availability: High		
Threat G 0.25 *Failure of devices or systems* (here: failure of the central administration server)	Core values impaired: Availability	
Frequency of occurrence without additional safeguards: Medium	Effects without additional safeguards: Considerable	Risk without additional safeguards: Medium

Database A1 Confidentiality: High Integrity: High Availability: High		
Threat G 0.32 *Misuse of authorisations*	Core values impaired: Confidentiality, integrity, availability	
Frequency of occurrence without additional safeguards: Rarely	Effects without additional safeguards: Threatening the existence of the organisation	Risk without additional safeguards: Medium

For the fictional company MUSTERENERGIE GmbH, a classification of risks (for the threats G 0.18 *Poor planning or lack of adjustment* and G 0.32 *Misuse of authorisations*) was carried out for the target object Smart Meter Gateway Administration Zx. The result can be obtained from the following table.

Smart Meter Gateway Administration Zx Confidentiality: High Integrity: High Availability: High		
Threat G 0.18 *Poor planning or lack of adjustment* (here: lack of or inadequate network segmentation)	Core values impaired: Availability, confidentiality, integrity	
Frequency of occurrence without additional safeguards: Frequently	Effects without additional safeguards: Considerable	Risk without additional safeguards: High

<table>
<tr><td>Threat

G 0.32 Misuse of authorisations</td><td colspan="2">Core values impaired:

Availability, confidentiality, integrity</td></tr>
<tr><td>Frequency of occurrence without additional safeguards: Frequently</td><td>Effects without additional safeguards: Considerable</td><td>Risk without additional safeguards: High</td></tr>
<tr><td colspan="3">etc.</td></tr>
</table>

6 Risk treatment

6.1 Risk treatment options

As already described in Section 5, different risk acceptance criteria are possible depending on an organisation's risk appetite. Below, it is assumed that an organisation accepts "Low" risks as a matter of principle, but "Medium", "High" and "Very high" risks only in exceptional cases.

In practice, the result of the classification of risks are, in most cases, several threats resulting in "Medium", "High" or "Very high" risks.

Therefore, a decision on how to deal with the *remaining risks* has to be taken. Suitable risk treatment options must be selected. Risks can

- avoided for example by excluding the cause of the risk
- be reduced by modifying the framework conditions which contributed to the classification of risks
- transferred by sharing the risks with other parties
- accepted, for example because the opportunities related to the risk are to be seized.

Below, the risk treatment options of avoidance, reduction and transfer are considered. Based on this, an organisation must define risk acceptance criteria and map the risk treatment on them. In all cases, the management must be involved in the decision how the risks identified are dealt with, because substantial damage or additional costs may result from the decision.

For every threat in the completed threat summary with the risk category "Medium", "High" or "Very high", the following questions must be answered:

A. Risk avoidance: Does it make sense to avoid the risk by restructuring the business process or the information system?

The reasons for such an approach may include:

- All effective countermeasures are associated with high efforts and thus very expensive, but the remaining threat cannot be accepted.
- Restructuring is appropriate for other reasons, such as reducing the costs.
- It can be easier and more elegant to change the existing procedures than to make them more complex by adding security safeguards.
- All effective countermeasures would be accompanied by substantial restrictions to the functions or comfort of the system.

B. Risk reduction (risk modification): Does it make sense and is it possible to reduce the risk by additional security safeguards?

The risk caused by the remaining threat might be lowered by developing and implementing one or several supplemental security safeguards which counteract the threat. The following sources of information on supplemental security safeguards may be useful:

- The manufacturer's documentation and support if the affected target object is a product
- Standards and "best practice" as prepared, for example, by information security committees
- Other publications and services, for example, those offered on the Internet or by specialised companies
- Experience gained within the organisation or at co-operation partners

The hypothetical effort and possible costs of any security safeguards required and information on existing security mechanisms are important decision-making aids.

C. Risk transfer (risk sharing): Does it make sense to transfer the risk to another organisation, for example by taking out an insurance policy or by means of outsourcing?

The reasons for such an approach may include:

- The potential damage is of a purely financial nature.
- The company already plans to outsource parts of the business processes for other reasons.
- For commercial or technical reasons, the contractual partner is better placed to handle the risk.

If additional security requirements are identified as part of the risk treatment, the risk classification (see examples below) must be adjusted for the target objects concerned. In this respect, it must be taken into account that new requirements might not only have effects on the respective target object analysed, but also on other target objects. The additional requirements and the security safeguards resulting from them are documented in the security concept.

If changes were made to the business processes or to the information system as part of the risk treatment, such as by means of risk avoidance or risk transfer, these changes must be taken into consideration in the security concept as a whole. In general, this also applies to work steps which are described in the IT-Grundschutz Methodology according to BSI Standard 200-2, starting with the structure analysis. Naturally, this may involve referring back to the information and documentation previously compiled.

For the transfer of risk, the appropriate form of contract is one of the most important aspects. Legal advice should be taken on this, particularly in the case of outsourcing schemes. The decision is taken by management and clearly documented.

D. Risk acceptance: Can the risks be accepted on the basis of comprehensible facts?

The risk classification and risk treatment steps are performed until the risk acceptance criteria of the organisation have been reached and the remaining risk (”residual risk”) is thus in accordance with the organisation’s objectives and specifications.

The residual risk must then be submitted to the management level for approval ("**risk acceptance**"). This documents in a traceable manner that the organisation is aware of the residual risk. Ideally, an organisation only accepts “Low” risks. In practice, however, this is not always appropriate. Reasons for also accepting higher risks may for example include:

- The respective threat only results in damage in very special circumstances.
- No effective countermeasures are currently known for the respective threat and in practical terms it is difficult to avoid.
- The effort and cost of effective countermeasures exceed the value of the asset to be protected.

Note:

Also those IT-Grundschutz requirements which are listed in the IT-Grundschutz Compendium as *requirements in the case of high protection requirements* as well as the related safeguards can be used as reference points for further security safeguards as part of a risk analysis. These are examples which go beyond the state-of-the-art level of protection and widely used in practice. It must be taken into account, however, that requirements in the case of high protection requirements are generally recommended, but not automatically binding even in the case of high security requirements. Therefore, they do not necessarily have to be involved in a risk analysis.

6.2 Risks subject to monitoring

In the risk analysis, threats might have been identified resulting in risks which are currently acceptable, but are expected to increase in the future. This means that there might be need for action in the further development. In these cases, it makes sense and is common to develop and prepare supplemental security safeguards in advance, which can be put into operation as soon as the risks become unacceptable.

These supplemental security safeguards must be documented and earmarked. The risks are monitored, and as soon as they are no longer acceptable, the earmarked supplemental security safeguards are checked, updated if necessary and included in the security concept. The risk classification is correspondingly adjusted according to Section 5. After the risk treatment has been completed for the remaining risks and the residual risks were accepted by the management level, the security concept can be completed for the information system under review.

However, in general, all risks should be monitored, i.e. not only those which are likely to increase in the future. To document the monitoring of the risks and adjustment of the safeguards and/or handling alternatives it is common practice to create a risk register or risk directories for this purpose.

For user-defined modules, the threats must be checked at regular intervals and evaluated again. Since the target objects covered by user-defined modules exceed the normal application of the IT-Grundschutz Compendium, the activities for monitoring risks described here must be taken into consideration in any case.

Example (excerpt):

For the threats identified in Section 5 with the risk category "Medium" or "High", the following decisions were taken:

Virtualisation Server S1 Confidentiality: High Integrity: High Availability: High		
Threat	Risk category	Risk treatment option
G 0.15 *Line tapping* (here: live migration)	Medium	D: Risk acceptance (risk assumption without additional safeguards) Only authorised administrators are allowed to access the live-migration network. They are trusted. The existing residual risk is assessed to be acceptable by RECPLAST and assumed.
G 0.25 *Failure of devices or systems* (here: failure of the central administration server)	Medium With supplemental safeguard: Low	B: Risk reduction Supplemental security safeguard: The central administration server is designed redundantly to ensure that the virtual infrastructure can still be operated without any problems in the case of a failure. The system is configured in such a way that, when an administration server fails, the system automatically switches to a backup server located in the cluster.

Database A1 Confidentiality: High Integrity: High Availability: High		
Threat	Risk category	Risk treatment option
G 0.28 *Software vulnerabilities or errors*	High With supplemental safeguard: Low	B: Risk reduction Supplemental security safeguard: The manual entry and approval of the hours worked would result in considerable extra effort on the part of the heads of departments and the personnel department, which cannot be achieved at the moment. Until the web application is replaced by a new application, a database firewall is used to reduce the existing risk. The database administrators create a suitable set of rules which prevent SQL queries injected at the web application from being executed on the database. The loss of performance which results from using a database firewall for the web application is assessed as tolerable.

Database A1 Confidentiality: High Integrity: High Availability: High		
Threat	Risk category	Risk treatment option
G 0.32 *Misuse of authorisations*	Medium With supplemental safeguard: Low	B: Risk reduction Supplemental security safeguard: In order to reduce the existing risk, an additional module of the database management system with which administrative accesses to critical data in databases are prevented is purchased. Moreover, actions of administrator IDs are securely logged and evaluated so that attempted violations can be detected at an early stage.

Smart Meter Gateway Administration Zx Confidentiality: High Integrity: High Availability: High		
Threat	Risk category	Risk treatment option

G 0.18 *Poor planning or lack of adjustment* (here: lack of or inadequate network segmentation)	High With supplemental safeguard: Low	B: Risk reduction Supplemental security safeguard: In order to reduce the existing risk, the smart meter gateway infrastructure is adequately segmented. IT systems on which the user interface of an SMGW Admin Software is operated are operated in a separate subnetwork. This is designed in such a way that it only has the minimum network couplings and communication connections necessary and to be established as compared to other subnetworks. In order to logically separate network segments from each other, firewalls are used.
G 0.32 *Misuse of authorisations*	High With supplemental safeguard: Low	B: Risk reduction Supplemental security safeguard: In order to reduce the existing risk, a role and rights concept which complies with the principles of the separation of functions and only grants access to authorised persons is implemented and documented. In the concept, a suitable separation of roles was also ensured. Furthermore, the concept also covers site access, system access, and data access authorisations.
etc.		

7 Consolidation of the security concept

If additional security safeguards must be added to the security safeguards already described in the security concept when treating the remaining threats, the security concept must subsequently be consolidated. Specifically, this means checking the security safeguards for each target object using the following criteria:

Suitability of security safeguards to counteract threats

- Have all the aspects of the relevant threats been covered in full?
- Do the counteractions match the security objectives?

Interaction of security safeguards

- Do the safeguards support each other in counteracting the relevant threats?
- Is an effective entity produced by the interaction of the safeguards?
- Do the safeguards conflict with each other?

User friendliness of security safeguards

- Are the safeguards tolerant towards user and operating errors?
- Are the safeguards taken transparent for the employees and other parties concerned?
- Is it clear to the users if a safeguard is omitted?
- Is it too easy for users to circumvent the safeguard?

Appropriateness/quality assurance of security safeguards

- Are the safeguards appropriate for the corresponding threats?
- Are the costs and effort required for implementation appropriate in scale for the protection requirement of the affected target objects?

The security concept should be adjusted and consolidated on this basis:

- Inappropriate security safeguards should be rejected and after a detailed analysis replaced by effective safeguards.
- Contradictions or inconsistencies in the security safeguards should be resolved and replaced by homogeneous mechanisms that are coordinated with each other.
- Security safeguards that are not accepted by the parties concerned have no effect. Practical solutions that restrict or hinder the parties concerned as little as possible should be found.
- Security safeguards that are too difficult or costly should be re-worked or rejected and replaced by appropriate safeguards. On the other hand, safeguards that are too weak endanger information security. They should also be reworked or replaced.

Integration of contents

- For target objects which are already included in the IT-Grundschutz Compendium, it can turn out to make sense to supplement existing modules by requirements determined in the risk classification.
- For target objects which cannot be mapped adequately with existing IT-Grundschutz, consideration can be given to summarising the new threats and requirements found (see examples for Smart Meter Gateway Administration, Section 4 and 5) in a user-defined module.

Example (excerpt):

When consolidating the security concept for RECPLAST GmbH, the following issues were found:

- Two years ago, it was decided that the use of encryption for network communications was not essential. A joint project group with the customer has reached the conclusion that this decision is no longer in accordance with the state of technology. Therefore, the requirements for configuring the router will be reworked in the short term and adjusted to the current needs.

  Both the Client C1 and the Switch N3 are used in the production area. As part of the risk analysis, it was found that the greatest threats to C1 result from air pollution, water splashes and vibrations. In the scope of a brainstorming session, it was thus decided to use an industrial PC which is particularly protected against physical threats instead of a commercially available PC. The industrial PC must be suitable for installation in standard 19 inch racks. Moreover, it must be equipped with an integrated or fold-out display as well as an easily exchangeable air filter and provide protection against splash water and vibrations.

- The requirements mentioned above take the special infrastructural framework conditions of Client C1 into account. In addition to this client, other information technology is being operated in the production area which is not the subject of the risk analysis but must be duly protected nonetheless. The company is taking the fulfilment of the requirements above as an opportunity to develop a policy governing the safe operation of information technology in the production area.

- etc.

Example (excerpt):

When consolidating the security concept for the administration of the Smart Meter Gateways, it was decided to summarise the threats determined as part of the risk classification and treatment.

- G 0.18 *Poor planning or lack of adjustment,*
- G 0.30 *Unauthorised use or administration of devices and systems,*
- G 0.43 *Importing of messages*
- etc.

and the security requirements and safeguards

- Suitable network segmentation
- Use of an adequate role and rights concept
- etc.

in one user-defined module.

8 Feedback to the security process

Once the security concept has been consolidated, the security process, as specified in BSI Standard 200-2 *IT-Grundschutz Methodology* (see [BSI2]), can be resumed. Therefore, the supplemented security concept becomes the basis for the following work steps:

- **IT-Grundschutz check** (see Section 7.7 and 8.4 of the IT-Grundschutz Methodology). An IT-Grundschutz check has already been performed as part of the preliminary work for the security requirements to be met under the IT-Grundschutz model. Since the risk analysis generally produces changes in the security concept, the subsequent implementation status of additional and altered requirements must be checked. If necessary, outdated results should be updated.
- **Implementation of the security concept** (Section 9 of the IT-Grundschutz Methodology). The security requirements provided in the security concept for the individual target objects must be met. To achieve this, the security safeguards derived from this must be implemented in practice so that they can become effective. Amongst other things, this includes estimating costs and expenses and deciding on the order of implementation.
- **Reviewing the IT security process on all levels** (see Section 10.1 of the IT-Grundschutz Methodology). In order to maintain and continuously improve the information security, the fulfilment of the security requirements and suitability of the security strategy must be reviewed among other things. The results of the reviews are incorporated in the updates of the security process.
- **The flow of information in the information security process** (see Section 5.2 of the IT-Grundschutz Methodology). In order to achieve traceability, the security process must be documented on all levels. This also particularly includes clear regulations for reporting channels and information flows. The management level must be informed about the status of the information security by the security organisation at regular intervals and in an adequate manner.
- **ISO 27001 certification on the basis of IT-Grundschutz** (see Section 11 of the IT-Grundschutz Methodology). In many cases, it is desirable to make the value of information security and the successful implementation of IT-Grundschutz in a public agency or company transparent. In this case, an *ISO 27001 certification on the basis of IT-Grundschutz* can be used.

9 Appendix

9.1 Risk appetite (readiness to take risks)

Risk appetite refers to an organisation's tendency how risks are assessed, evaluated and dealt with. This tendency results from cultural, internal, external or economic influences.

The tendency within an organisation to take risks is influenced by a variety of factors so that classifying of the risk appetite quantitatively can become quite complex. This section aims at reducing the complexity and defining a manageable number of risk appetite types for which recommendations for handling risks in a reasonable manner can be given.

9.1.1 Influencing factors

External conditions which influence the risk appetite of an organisation include:

- Cultural influences (depending on the country and mentality, the readiness to take risks differs)
- Internal factors (organisational culture, attitude of the management of understanding risks as a problem or opportunity)

  Conservative organisations rather tend to avoid risks (e.g. government authorities or companies which strive towards a particularly serious image). Quickly growing companies are rather willing to take risks, whereas established large-scale companies tend to avoid risks. In the case of large-scale companies, however, it makes sometimes also sense to set up risk management for different company departments differently depending on whether the areas are new, technology-intensive areas (with a high risk appetite) or "cash cows" (with a low risk appetite). Large-scale companies have the advantage that they can spread risks over different areas. Therefore, the risk appetite can also vary in different parts of the company. The clearer the visions and strategic objectives of the organisation are, the more directly this will result in an attitude towards risks.
- Market environment (e.g. conservative or innovative environment)

  Market environment and internal factors are closely related to each other. The one who enters new markets must adopt to the rules applicable there and to competition in particular even if this might be contrary to the organisation's tradition. It makes sense to observe competing organisations and to adjust one's own course of action (e.g. according to the rules of the game theory) accordingly. The strategy can (here, in turn, depending on the culture within the organisation) be to be the leader of the market: In this case, it will be necessary to demonstrate readiness to take high risks. In the other case, the organisation can decide to act as a "fast follower". This means that it tries to leave the risks to the competitors and to still gain an attractive share of the market. When deciding whether an organisation implements specific safeguards or not, it also often matters what the competitors are doing (provided that their safeguards are known).
- Risk-bearing capability (financing of the organisation (liability, capital cover etc.))

  Although large-scale companies, as already mentioned, rather tend to avoid risks, they usually have a capital cover which allows it at least in individual areas to bear risks. Small-scale companies which rather have a low capital cover, but still have to take significant risks for reasons of the market environment sometimes cooperate with venture capitalists for the same reason.

9.1.2 Quantification of risk appetite

In simple terms, the risk management consists of the following steps. Precise definitions can be found, for example, in ISO/IEC 31000 (see [31000]) or NIST SP 800-30 (see [NIST800-30]):

- Risk identification

- Risk assessment (determination of frequency of occurrence and extent of damage)
- Risk evaluation (determination of the risk category)
- Determination of safeguards for treating risks
- Comparison between the costs of every safeguard and the damage to be expected and decision in favour of or against the implementation of the safeguard
- Examination of the residual risks: Definition of handling options
- Comparison with opportunities (expected revenues and benefit of the field of business)
- Monitoring of the risks and adjustment of the safeguards or handling options during live operation

In several of these steps, the risk appetite of an organisation can be reflected.

Criteria for risk appetite

Trying to define criteria for the risk appetite leads to several possible approaches. The following are some examples:

- Highest possible acceptable risk
- Highest possible acceptable frequency of occurrence for risks
- Acceptance of risks with high market opportunities at the same time
- Acceptance of unpredictability (e.g. If it is very difficult to assign risks to a frequency or amount of damage)
- Selection of treatment alternatives as from a certain residual risk

It is not always possible to provide rational reasons for attitudes towards risks. An example would be an organisation's general aversion to take risks with a high frequency of occurrence, because if these risks would not be associated with high damage, they would not necessarily have to be avoided. Such a decision, however, could still be taken intuitively if the organisation is not sufficiently certain when determining the extent of damage. An analogue argument would be correct regarding the attitude towards a maximally accepted amount of damage. Imprecise data material results in organisations having to decide themselves in one or the other way. The decision is strongly influenced by the risk appetite.

Best possible strategy and uncertainty

If it were possible to exactly determine all parameters which are used in the risk management, it would also be possible to determine a way in which the risks are handled optimally. These parameters are for example frequencies of occurrences and amounts of damage (before and after treatment by means of safeguards), the costs of safeguards, the costs of treatment alternatives and the expected opportunities, i.e. for example revenues from a business transaction.

Risks must always be weighed against opportunities. It would be typical for example in the case of a field of business associated with risks that risk-averse organisations avoid the risk and, at the same time, miss the corresponding opportunity, whereas less risk-averse organisations take the risk, but thus seize the opportunity at the same time.

If it were possible to exactly determine all of the parameters mentioned above, a precise empirical value could be determined for the profits gained or losses of the organisation depending on whether the risk is taken or not. In this case, there would be one best possible strategy for the organisation and the question of the risk appetite would no longer play a role.

This clearly illustrates that the risk appetite is important, because the input data for the risk management is subject to uncertainty. The question is how the uncertainties are evaluated and how the organisation is prepared for a high case of damage.

Possible measures

Irrespective of rather intuitively justified risk appetites, as described above, an attempt is to be made to determine measures for the risk appetite. This attempt is based on the steps which were described above for the basic risk management procedure and a rational approach is to be aimed at when determining the risks.

The simplest measure is based on the empirical value for the extent of damage, defined as a product of the frequency of occurrence for the risk and the amount of damage. Risks are often shown as a matrix in which the frequency of occurrence is displayed on the one axis and the extent of damage on the other. The high risks can be found in a red coloured area in the matrix. "High risk appetite" could thus be defined in the simplest case as readiness to also accept risks in this area. "Low risk appetite" would mean avoiding risks, which also means possibly abstaining from seizing a revenue opportunity at the same time.

Figure 4 shows an exemplary risk matrix with defined risk categories.

In order to define the threshold values by means of which the frequencies of occurrence and the effects are classified as "High", organisations typically orient themselves by their financial figures. The management level decides which threshold values it classifies as "high". The threshold could be based on the financial reserves, but also on the turnover of the organisation. The threshold can be determined as a certain percentage of the turnover. However, it can also be based on the fact whether the organisation would still be solvent if a certain risk occurs. Depending on the height of the risk, decisions must usually be approved by different management levels and high risks should not be taken without the permission of the top management.

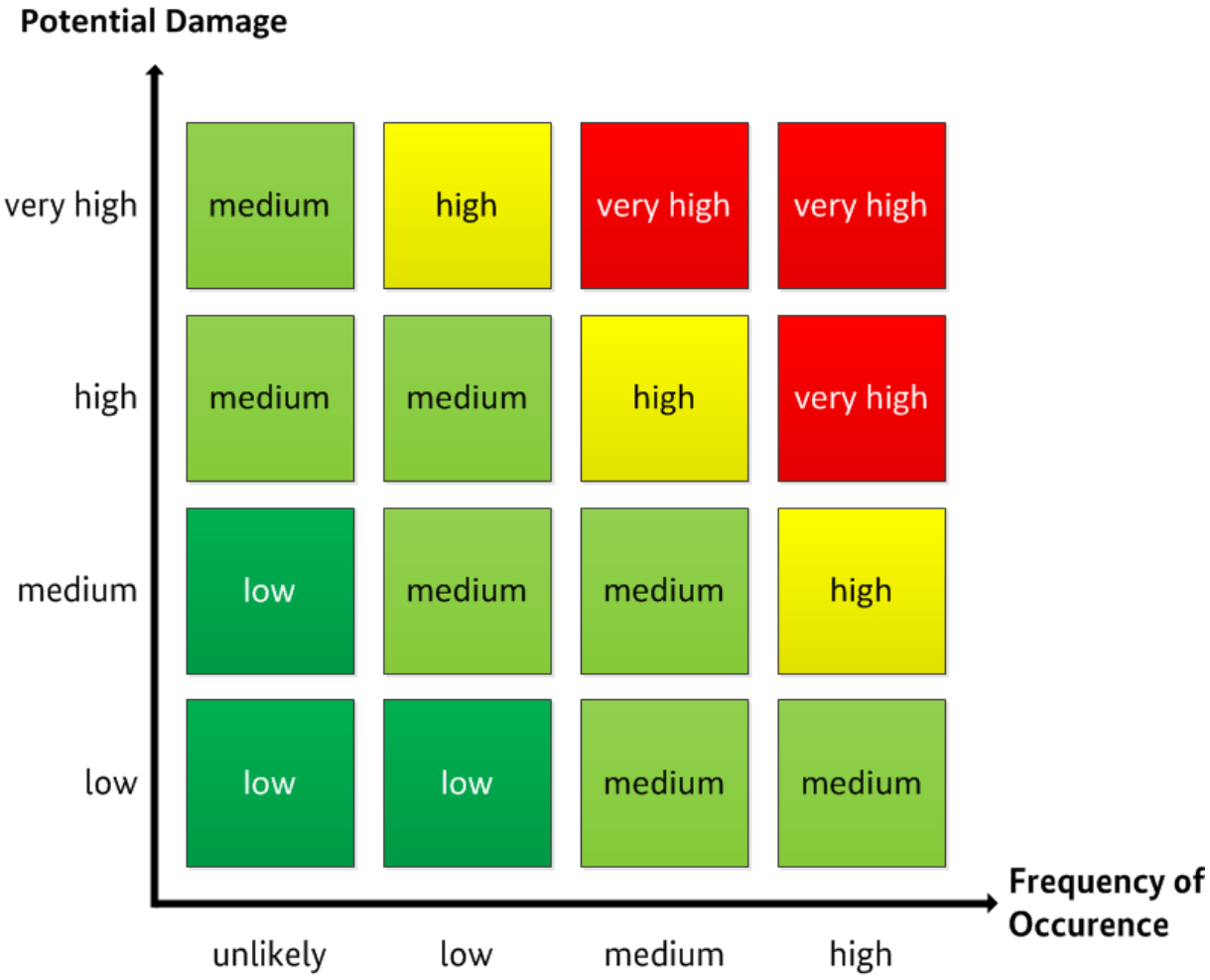


Figure 4: Exemplary risk matrix with risk categories

If risks are assessed and entered into the risk matrix shown above, the result is an illustration as in Figure 5 in which six different risks were determined and entered as circles with numbers. Here, an

organisation with a high risk appetite (upper of the two black lines) would bear the risks 1 and 3 below the line, whereas an organisation with a low risk appetite would only bear the risks 4, 5 and 6 (lower line). No organisation would take risk 2 in this case.

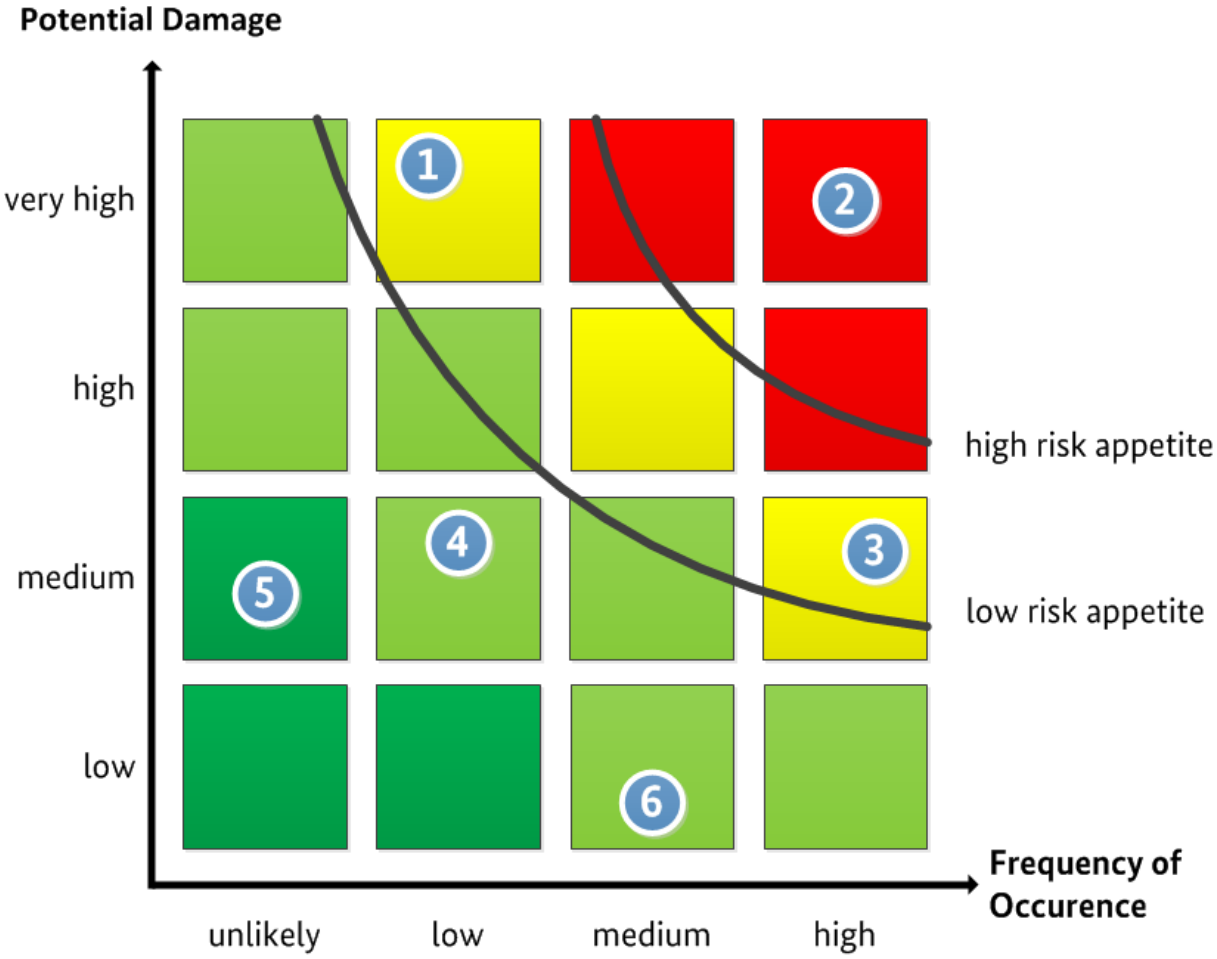


Figure 5: Risk matrix with risks entered

As already mentioned above, there would be no reason for organisations with a low risk appetite to forgo opportunities if reliable data gives reason to expect revenues which exceed the costs caused by risks occurred. Solely the uncertainties regarding the data collected are the reason why organisations with a lower risk appetite tend to avoid risks in such situations.

Another definition for risk appetite is accepting uncertainties regarding the interpretation of the data material. For innovative sectors in particular, organisations cannot fall back on much available data material when determining frequency of occurrence and the extent of damage of risks. Imponderabilities almost always come into play with respect to risks in the field of information security in contrast to risks which can be predicted statistically, such as for damage by the elements in the insurance industry.

The uncertainties can be displayed in a risk diagram for example with error bars representing the uncertainty of the data. The lengths of these error bars must be determined only intuitively where there is greater uncertainty.

Figure 6 shows a risk matrix with error bars. In this example, they have a vertical orientation, which means that they indicate an uncertainty with respect to the extent of damage. Error bars in horizontal orientation would equally be possible. In this diagram, organisations with a low risk appetite would rather orient by the upper edge of the values for the frequency of occurrence and the extent of damage, and organisations with a high risk appetite by the middle (not by the lower edge, because this would then mean to systematically underestimate risks).

It is interesting to compare the risks 4 and 5: An organisation with a low risk appetite would rather accept risk 4 than 5 in this situation, although it has a higher empirical value for the damage. Here, the uncertainty regarding the extent of damage is decisive, which is higher for risk 5, marked by the error bar which projects in a higher extent of damage for risk 5 than the one of risk 4.

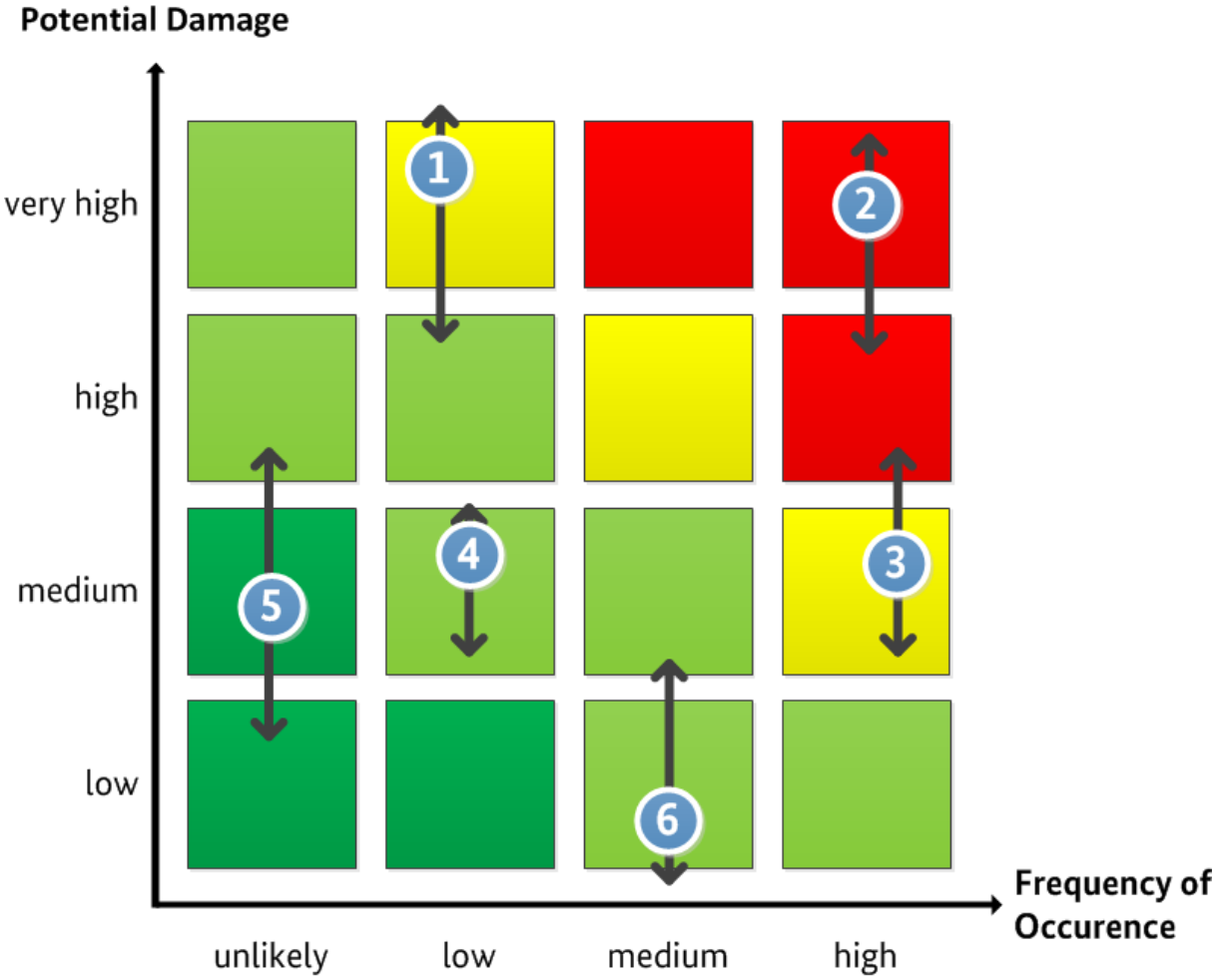


Figure 6: Risk matrix with uncertainties

Finally, it is also possible to group risks in different categories and to develop a different risk appetite per category. For example, an organisation could shy away from reputational damage, but be willing to take high financial risks. In principle, this does not change the procedure, but the different categories are simply considered separately.

Risk types

In a simple model, organisations can be divided into different types depending on how they handle risks. For example, the division could be as follows:

- The “Cowboy” – corresponds to an organisation which readily takes the risks in principle
- The “Risk eater” – takes high risks if they are also offset by high opportunities
- The “Conservative – tries to minimise all risks as far as possible by means of safeguards

If “Cowboy” refers to an organisation which simply ignores risks, this contradicts the principles of the risk management and it is hardly possible to make reliable statements regarding consequences to be expected, i.e. damage or opportunities.

For the following consideration, it is to be assumed that an organisation operates a professional risk management. Even professional risk management cannot always prevent that bad decisions are made, but it still ensures that the decision is taken deliberately on the basis of existing analyses. The risk

appetite should not have any influence on the decision whether a risk analysis is performed at all and how carefully this analysis is carried out. However, it may influence how many resources are invested by the organisation in the risk analysis and treatment. This should be a deliberate decision.

In the remainder of this section, the following categories are used:

- The conservative

  The conservative shies from risks which are in red (and maybe also in the yellow) area of the risk matrix (see Figure 4) and avoids them. The opportunities associated with this are too uncertain for them in order to get involved with the threats.

- The risk-affine

  The risk-affine always sees the opportunities which are associated with high risks. If they are promising, but only then, they are willing to take the risk. Organisations taking any risk even if these risks are not offset by equal opportunities act in a self-destructive manner and will not be dealt with further below.

- The uncertainty avoider

  The uncertainty avoider tries to collect as reliable data as possible on their risks. They rather tend to avoid risks if it is difficult to assess them quantitatively than if they are high, but can be controlled well and covered by solid financing or the revenues to be expected. In the latter case, they differ from the conservative.

9.1.3 Risk appetite as input variable in the ISMS

As the risk analysis is an important component of the ISMS, the basic prerequisites for this should be defined by the management of the organisation. The management level specifies the risk appetite. The security management must know the risk appetite and implement it accordingly.

An organisation might not be aware of its own risk appetite or has only a vague idea of this term. In this case, the management should provide clarification and take a decision with the advice of a specialist (e.g. by the information security officer (or ISO) or risk manager) if necessary. The influencing factors mentioned above are taken into consideration. The organisational unit responsible for the requirements management (corporate compliance) should also be consulted.

The management’s statement regarding the risk appetite can be specified in more detail at the beginning of the risk analysis within the meaning of the categories or measures defined above. It is important to regularly check this specification and adjust it to the objectives of the organisation on the one hand and, on the other, to implement it consequently for risk analyses and treatment. Cases of doubt may arise for example if it does not make sense to apply the risk appetite defined for a certain risk. Those exceptional cases should be coordinated and documented.

It was described above which aspects can be influences by the risk appetite. If decisions which were influenced by the risk appetite, among other things, are taken, this should be documented.

As soon as the risks have been assessed and evaluated, a possible treatment of these risks should already be considered based on the given risk appetite before supplemental security safeguards are determined. Under certain circumstances, it is not worth planning supplemental security safeguards. In the opposite case, security safeguards are planned and evaluated to reduce the risk, and the residual risk is evaluated afterwards. Residual risks must be treated, if they go beyond the accepted risk. The risk appetite is considered once again in the decision in favour of a treatment option.

When deciding whether a risk is to be borne by oneself or transferred, "the risk-affine" will rather tend to the first option, whereas "the conservative" and "the uncertainty avoider" types will rather tend to the second option, although generalised statements are not always true. The "uncertainty avoider" may try to reduce the uncertainty regarding the risk assessment by implementing safeguards under their own control.

With the individual decisions which are taken in the risk analysis and treatment, it is also recommended to document the influence of the risk appetite on these decisions. When the risk appetite has been changed (e.g. due to changed market conditions), the risk analysis can be adjusted more easily.

Moreover, the risk appetite has an impact on the organisational structure of an organisation. One example is the question whether there is an organisational unit for the risk management and how it is composed, although this decision is of course also influences by factors such as the size of the company.

As a matter of principle, the following is recommended: The one who committed to a high risk appetite ("the risk-affine" type) should take this into account in their risk management process and their organisational structure. High risks require careful monitoring and control.

9.1.4 Effect of laws and regulations

Laws and standards do not influence the risk appetite of an organisation itself, but the way they deal with risks. The risks increase due to regulatory pressure so that the balance between risk appetite and original risks can shift. Every organisation must include sanctions due to legal or contractual breaches in their risk calculation.

An example of legislation influencing the risk management of companies are data protection acts. In numerous companies, breaches in the handling of personal data occurred despite of preventive safeguards. Against the backdrop of these experiences, this should be taken into consideration in the risk management. It is particularly important to localise the errors resulting in data protection violations and to derive and implement suitable safeguards. For example, training of employees and awareness campaigns come into question.

There are many examples of regulations by supervisory authorities, for example in the banking industry. Decisions of an organisation to take risks in any case, although the capital cover would not be sufficient when reviewed seriously are prevented by provisions of financial supervision or corresponding sanctions imposed.

9.2 Moderation of the risk analysis

For performing a risk analysis, specialists responsible and/or experts for the respective target objects under review must be involved. In practice, it has proved to be successful to better perform several short sessions than one long session with all employees involved. Information security officers, specialists responsible, administrators and users of the target object under review as well as external experts, if appropriate, should be involved.

A moderator should be appointed. The participants' objectives should be clearly formulated and the time for the sessions limited.

To ensure that the decisions required for the respective steps of the risk analysis can directly be consolidated, e.g. with respect to risk acceptance, costs and feasibility, a representative of the management level should be present (at least towards the end).

The team should not be too large (4 to 8 persons have proved to be successful). The team should have sufficient expertise for all aspects of the area under review.

- The moderator should already have participated in risk analyses so that they are familiar with the procedure.
- The meeting should take place under framework conditions allowing the participants to work in an undisturbed manner, as high concentration is required.
- The field of analysis should be defined clearly.
- A clear standard for the evaluation of risks must be defined to ensure that all risks are treated at the same level and the safeguards taken are comparable and comprehensible.

- All participants should be familiar with the rough framework of the risk analysis and the area under review so that they could think about threats, effects of damage and safeguards in advance. This also includes that they know the objects belonging to the area under review as well as the related business processes, backgrounds, embedding in the organisation and the technology as well as technical principles.
- All threats coming into the participants' minds should also be mentioned and discussed. The moderator is responsible for ensuring that finding the results is not lost sight of during the discussions.
- Detailed questions requiring special expertise should be prepared in advance. Individual aspects can also be clarified subsequently.
- A result report should be drawn up. As many potential points of attack were discussed, the documents should be treated confidentially.

There should be clear time constraints for the implementation of each risk analysis. Experience has shown that the results become the better, the more systematically and concentrated the analysis is performed, and not the longer it takes. A risk analysis for complex issues can usually also be completed in one day. If the area under review is too comprehensive, however, it should be divided into different sections. For a risk analysis, too, the 80:20 rule should be observed. Since it is not possible anyway to review any possible issue, the most probable threats and most plausible solutions should always be focused on. If esoteric threats are discussed, i.e. those which are extremely rare and highly unlikely, this is sign that the concentration needed is no longer available.

9.3 Determination of additional threats

The following issues should be considered when determining additional threats:

- Which *force majeure* events represent particular threats for the information system?
- Which *organisational failures* must be avoided in order to guarantee information security?
- Which *human errors* can particularly impair the security of the information?
- Which special security problems could occur to the target object under review due to *technical failure*?
- Which particular threats arise from deliberate attacks by *outsiders*? This refers to people that are not part of the organisation itself and have no access to internal resources through special arrangements.
- How can *insiders* affect the proper, secure operation of the target object under review through deliberate actions? Particular threats frequently arise as a result of existing access authorisation and insider knowledge.
- Are there special threats caused by objects which cannot be attributed to the information system considered? Those *external objects* can for example be foreign applications, IT systems or structural situations. The definition of the information system considered is used to specify the subject under examination for the security concept. However, this must not lead to neglecting threats posed from outside the information system under review when carrying out the risk analysis. Such sources of special threats may include
    - The manufacturer's documentation
    - Warning and information services of Computer Emergency Response Teams (CERTs), such as that of the BSI at https://www.cert-bund.de
- Publications about vulnerabilities on the Internet and (e.g. Threat Intelligence, Feeds) and one's own threat analyses.

9.4 Interaction with ISO/IEC 31000

In the international standards on risk management and risk determination, in particular in ISO/IEC 31000, some terms are used with a different meaning than in this standard. The following table compares the most important terms of ISO/IEC 31000 and BSI Standard 200-3. The purpose of this comparison is to facilitate the assignment of the terms of ISO 31000 to the terms in the BSI Standards 200-2 and 200-3 (see Figure 7).

ISO/IEC 31000 and IT-Grundschutz

ISO/IEC 31000:2009	IT-Grundschutz
Establishing the context, Section 5.3	**BSI Standard 200-1** (see [BSI1]), Management principles, Section 4 Planning the security process, Section 7.1 **BSI Standard 200-2:** Initiation of the security process, Section 3
Risk assessment, Section 5.4 • Risk Identification • Risk Analysis • Risk Evaluation	**BSI Standard 200-3** Risk determination, Section 1 • Drawing up of a threat overview • Risk assessment • Risk evaluation
Risk identification, Section 5.4.2	**BSI Standard 200-3:** Drawing up of a threat overview, Section 4
Risk analysis, Section 5.4.3	**BSI Standard 200-3:** Risk assessment, Section 5.1
Risk evaluation, Section 5.4.4	**BSI Standard 200-3**, Risk evaluation, Section 5.2
Risk treatment, Section 5.5	**BSI Standard 200-3**, Risk treatment, Section 6
Communication and Consultation, Section 5.2	**BSI Standard 200-1**, Communication and knowledge, Section 4.2 **BSI Standard 200-2:** Information flow in the IT security process, Section 5.2
Monitoring and review, Section 5.6	**BSI Standard 200-1:** Maintaining information security, Section 7.4 Continuous improvement of the information security, Section 7.5 **BSI Standard 200-2:** Maintenance and continuous improvement of the information security, Section 10 **BSI Standard 200-3:** Risks subject to monitoring, Section 6.2

Table 10: Comparison of terms from ISO/IEC 31000 and BSI Standard 200-3

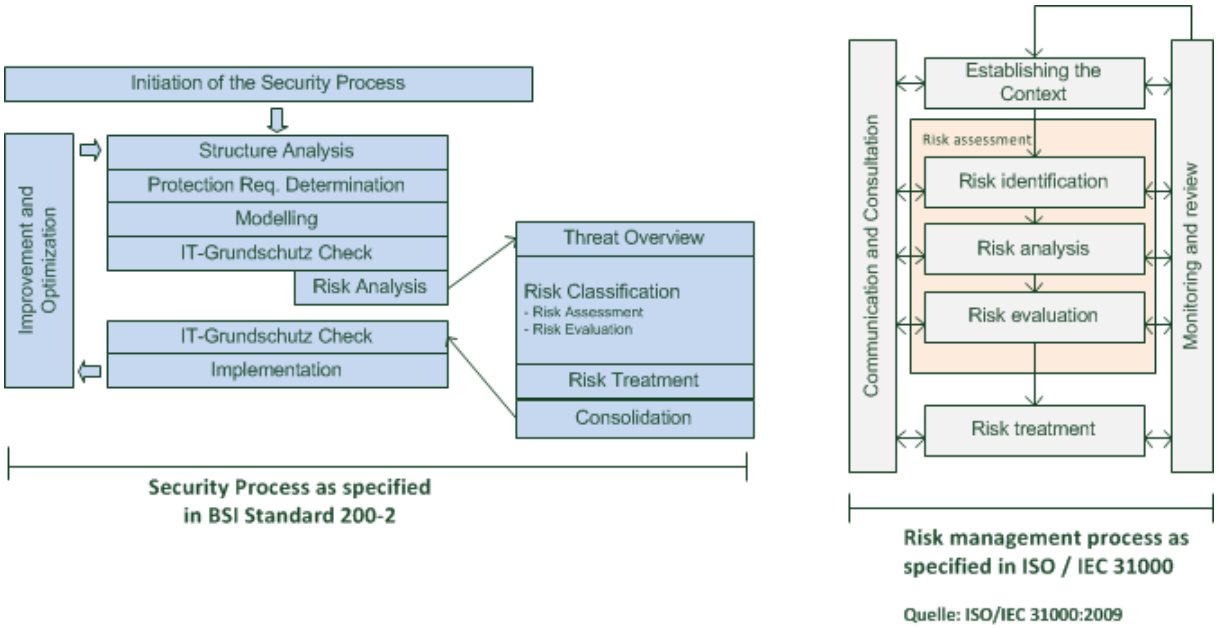


Figure 7: Security process according to BSI Standard 200-2 and risk management process according to ISO/IEC 31000

9.5 References

[27005] ISO/IEC 27005:2011, International Organization for Standardization (ed.), Information technology — Security techniques — Information security risk management, ISO/IEC JTC 1/SC 27, 2011

[31000] ISO/IEC 31000:2009, International Organization for Standardization (ed.), Risk management — Principles and guidelines, ISO/TC 262, 2009

[31010] ISO/IEC 31010:2009, International Organization for Standardization (ed.), Risk management — Risk assessment techniques, ISO/TC 262, 2009

[BSI1] Information Security Management Systems, BSI Standard 200-1, Version 1.0, October 2017, https://www.bsi.bund.de/grundschutz

[BSI2] IT-Grundschutz Methodology, BSI Standard 200-2, Version 1.0, October 2017, https://www.bsi.bund.de/grundschutz

[BSI4] Business Continuity Management, BSI Standard 100-4, Version 1.0, November 2008, https://www.bsi.bund.de/grundschutz

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

[ISACA] Leitfaden ISO 31000 in der IT mit Vergleich zu anderen Standards, ISACA German Chapter e.V. und Risk Management Association e.V., June 2014, https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/attachements/2014_11_isaca-leitfadenanwendungderiso31000inderit.pdf

[Koenigs] IT-Risikomanagement mit System – Praxisorientiertes Management von Informationssicherheit und IT-Risiken, Hans-Peter Koenigs, Springer, 2013

[NIST800-30] Guide for Conducting Risk Assessments, NIST Special Publication 800-30, September 2012, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[SHB] IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik, BSI, Version 1.0 – March 1992, Bundesdruckerei