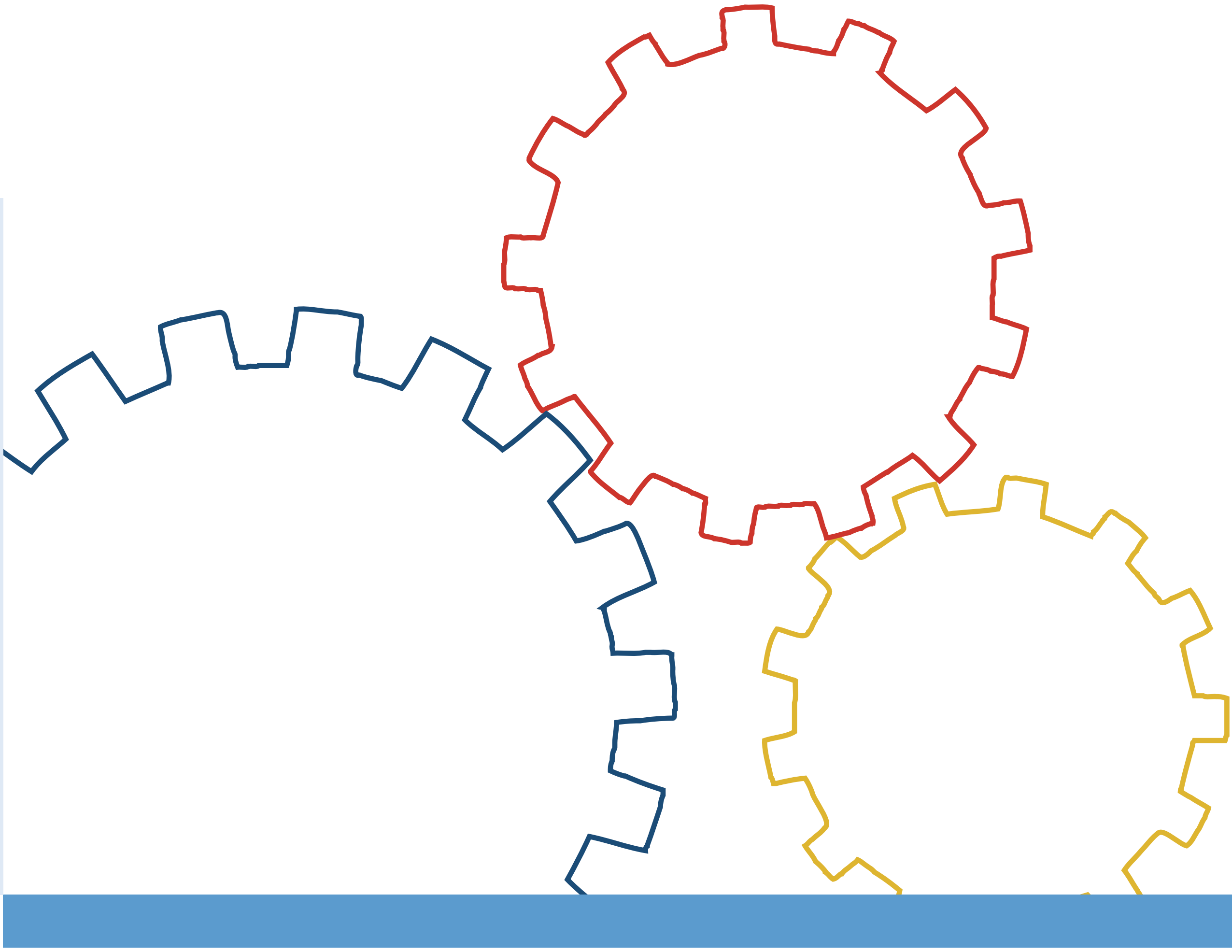
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 100-3

Risk analysis based on IT-Grundschutz



www.bsi.bund.de/grundschutz

Version 2.5

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189, 53175 Bonn

Contents

1. Introduction

1.1 Version history

As per	Version	Changes
February 2004	1.0	
December 2005	2.0	• Adapted to BSI Standard 100-2
May 2008	2.5	• Stronger emphasis on the information security instead of the IT security, resulting in the modification of various terms • Modified to reflect the new structure and organisation of BSI-Standards 100-2 • To avoid confusion with the Z-safeguards from the IT-Grundschutz Catalogues, the term "supplementary safeguards/security safeguards" is used instead of the term "additional safeguards" throughout the document. • Explicit presentations of the threats from external objects in Chapter 4 • Uniform treatment of the OK status of threats • Added Section 6.2 which deals with the subject of "Risks under examination"

1.2 Aims

The methodology outlined below demonstrates how the threats listed in the IT-Grundschutz Catalogues [GSK] can be used to carry out a simplified analysis of risks for information processing. Examples of potential areas of application for an analysis of this kind in public agencies and companies include target objects which

- Have a high or very high security requirement in at least one of the three basic parameters of confidentiality, integrity or availability
- Cannot be adequately mapped (modelled) with the existing modules of IT-Grundschutz
- Are operated in scenarios (environments, applications) which are not covered by IT-Grundschutz

In these cases the following questions arise:

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

This document outlines a methodology for determining, for specific targets and for as little effort as possible, whether and in what respect there is any need to take action over and above the IT-Grundschutz in order to contain risks for information processing.

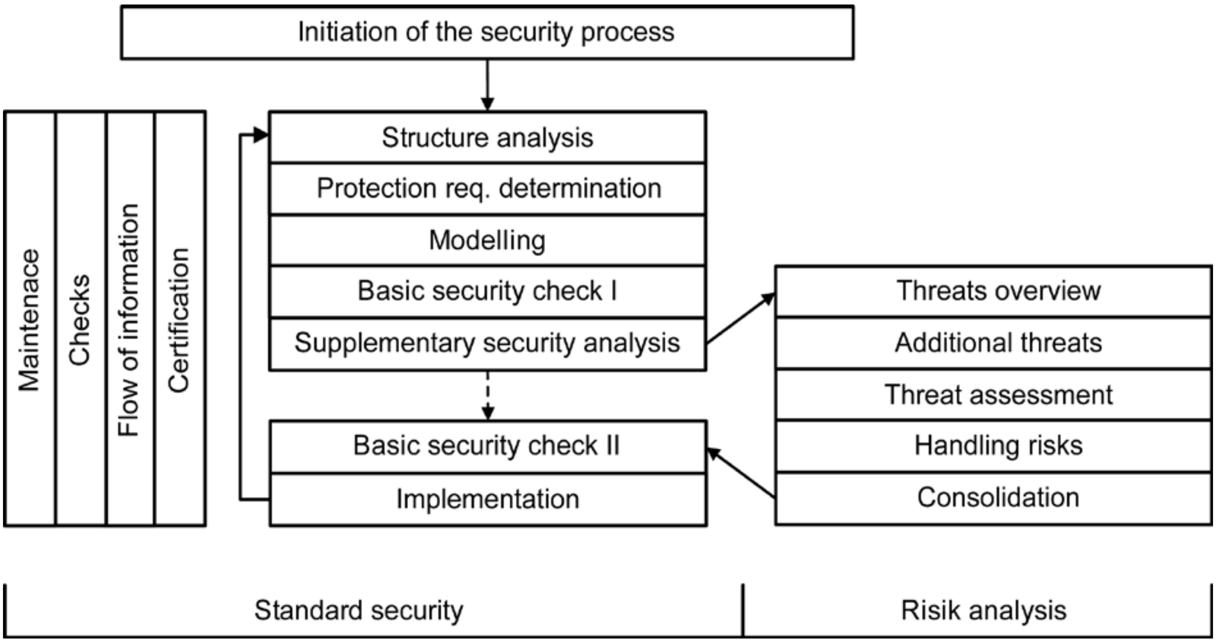


Figure 1: Integration of the risk analysis into the security process

The "IT-Sicherheitshandbuch" [SHB] and other approaches to analysing risks and security include such issues as the probabilities of occurrence in order to take decisions on how to handle the threats. But it has been proven that assessing the probability is often difficult in practice because there is no basis for reliable estimates. The interpretation of the probabilities is also frequently questionable. Therefore, in the methodology described here, the probabilities of occurrence is not considered explicitly but rather implicitly as part of determining and assessing the threats.

1.3 Target group

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

Those using the methodology outlined in this document should be familiar with the IT-Grundschutz Methodology according to BSI Standard 100-2 [BSI2].

1.4 Application

This document outlines the methodology for carrying out risk analyses to supplement an existing IT-Grundschutz security concept. The document draws on the threats specified in the IT-Grundschutz Catalogues.

It is recommended to carry out the procedure described in Sections 2 to 8 step by step.

1.5 References

[BSI1] Information Security Management Systems (ISMS), BSI Standard 100-1, Version 1.5, May 2008, www.bsi.bund.de

[BSI2] IT-Grundschutz Methodology, BSI Standard 100-2, Version 2.0, May 2008, www.bsi.bund.de

[BSI3] Risk Analysis on the Basis of IT-Grundschutz, BSI Standard 100-3, Version 2.5, May 2008, www.bsi.bund.de

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

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

2 Preliminary work

Before starting the actual risk analysis, the following preliminaries should have been dealt with, as specified in BSI's IT-Grundschutz Methodology according to BSI Standard 100-2 [BSI2]:

- A systematic *information security process* must *have been initiated*. This serves to channel the information security operations along ordered tracks. For example, appropriate roles and tasks must be defined. Further information on introducing the information security process can be found in Section 3 of the IT-Grundschutz Methodology.
- In accordance with Section 4.1 of the IT-Grundschutz Methology a **scope** for the security concept *must be defined*. This area of application is referred to in the following as the *information domain*.
- A *structure analysis* must have been performed for the information domain, as specified in Section 4.2 of the IT-Grundschutz Methodology. This is a way of ascertaining the key information about the information domain, for example the basic network layout and a list of the most important applications which depend on the IT systems.
- Subsequently, an *assessment of protection requirements* must have been performed, as specified in Section 4.3 of the IT-Grundschutz Methodology. The result is the protection requirement for the applications, systems, rooms used by the IT assets and a list of the critical communication links. The security requirement refers to the basic parameters of *confidentiality*, *integrity* and *availability* and is determined at three levels, namely *normal*, *high* and *very high*.
- A *modelling process* must have been performed, as specified in Section 4.4 of the IT-Grundschutz Methodology and Section 2 of the IT-Grundschutz Catalogues. This involves determining which target objects in the information domain each module of the IT-Grundschutz Catalogues should be applied to. The standard security measures stated in the individual modules form the basis for the IT-Grundschutz security concept for the information domain under review.
- Prior to the risk analysis a *basic security check* must be performed, as specified in Section 4.5 of the IT-Grundschutz Methodology. This determines which standard security measures have already been implemented for the information domain under review and where there are still deficits.
- A *supplementary security analysis* must have been performed, as specified in Section 4.6 of the IT-Grundschutz Methodology. During the Supplementary Security Analysis a decision is made as to which objects are to be the subject of risk analyses and to identify those for which this is not necessary.

The objects which have been earmarked for risk analysis during the supplementary security analysis are referred to below as the target objects under review or components under review.

Example:

A supplier maintains a communication link to his main customer. The customer uses this link to notify the supplier about current needs for products in particular colours, sizes and types continuously. In order to minimise the data volume only changes to previously notified requirements are transmitted. The supplier uses these notifications of requirements as the basis for assigning production capacities. In this manner it is guaranteed that the supplier produces and supplies each of the quantities of the individual colours, sizes and types as precisely as possible.

In technical terms the communication link is implemented via a rented fixed line to the main customer. A failure of just two hours can result in substantial over-production or supply bottlenecks and therefore high costs to the company. The following sub-section of the whole information domain therefore has a high protection requirement in terms of availability:

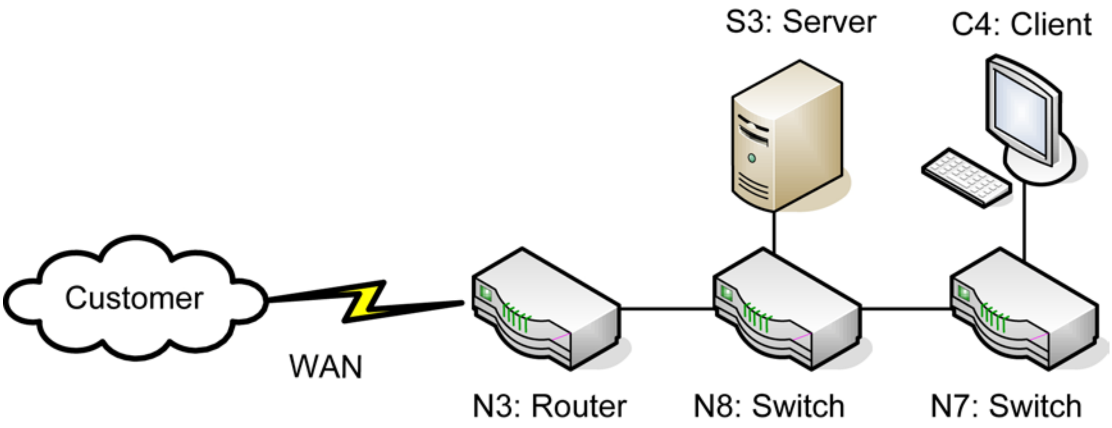


Figure 2: Part of a network as example for high protection

The affected components are located in Rooms M.723 (server room), M.811 (technical room) and E.5 (production area control room). The supplementary security analysis entailed the decision that no risk analysis is required for any other components with a high protection requirement.

3 Preparing the threat summary

The threats which are relevant to the target objects under review and are listed in the IT-Grundschutz Catalogues constitute an appropriate starting point for the risk analysis. In contrast to the "IT-Sicherheitshandbuch" [SHB], threats, vulnerabilities and risks are not examined separately here.

The aim of the following work steps is to produce a summary of the threats to which the target objects under review are subject. For this purpose it is advisable to initially reduce the information domain down to the components under review.

1. After modelling the information domain, the first target objects or groups of target objects to be deleted are those which were identified in the supplementary security analysis as not requiring risk analysis. This means that all target objects not under review are eliminated from the modelling process.

   Example: (Excerpt)

No.	Title of module	Target object	
B 2.3	Office	~~Room M.501~~	delete
B 2.4	Server room	Room M.723	
B 2.6	Technical Infrastructure Room	Room M.811	
B 3.101	General server	~~S2~~	delete
B 3.101	General server	S3	
B 3.102	Server under Unix	~~S2~~	delete
B 3.102	Server under Unix	S3	
B 3.201	General Client	~~C2~~	delete
B 3.201	General Client	C4	
B 3.301	Security Gateway (Firewall)	N3	

2. Subsequently, all the modules that remain in the table for which there is no target object or group of target objects left are deleted. These modules are evidently irrelevant to the target objects under review.

   In general, it is only possible to remove objects in layers 2 to 5 because the modules in layer 1 usually relate to all or at least many target objects. In some cases modules may be removed from layer 1 if it is clear that the issue handled by the module is irrelevant to the corresponding risk analysis.

   Examples:

   - The module B 1.3 *Contingency Planning Concept* and B 1.8 *Handling Security Incidents* can be dispensed with in the majority of cases if the risk analysis only deals with sub-areas which have a normal level security requirement for availability.
   - It is usually possible to remove the module B 1.7 *Encryption concept* if the risk analysis only handles sub-areas that have a normal protection requirement for confidentiality and integrity.

   The result of these steps is a table in which the modules that are relevant for the target objects that have a high protection requirement are listed. The modules in layer 1 are important for all or many target objects; in contrast, the modules in the other four layers refer to special target objects or groups of target objects.

Example: (Excerpt)

No.	Title of module	Target object
B 2.4	Server room	Room M.723
B 2.6	Technical Infrastructure Room	Room M.811
B 3.101	General server	S3
B 3.102	Server under Unix	S3
B 3.201	General Client	C4
B 3.301	Security Gateway (Firewall)	N3

3. Each module from the IT-Grundschutz Catalogues refers to a list of threats. For each target object in the table the number and title of these threats are inserted from the modules and assigned to the relevant target object. It is useful in this case to handle the threats in the modules in Layer 1 separately by assigning them to the special target object "entire information domain", for example.

4. The result is a table that assigns a list of relevant threats to each target object. All duplicates and multiple copies of threats for each target object should be removed from this table.

5. Subsequently, the threats in the table should be sorted for each target object by subject. Some threats in the IT-Grundschutz Catalogues deal with similar security problems or with different forms of the same threat (e.g.T 1.2 *IT System Failure* and T 4.31 *Failure or Malfunction of Network Components*).

6. 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 ranking target object of the *entire information domain*.

   This table presents a *threat summary* for the target objects under review. It serves as the initial point for the subsequent *determination of additional threats*.

Example: (Excerpt)

Communication server S3	
Confidentiality:	Normal
Integrity:	High
Availability:	High
T 1.2	Failure of the IT system
T 3.2	Negligent destruction of equipment or data
T 4.1	Disruption of power supply
T 5.57	Network analysis tools
T 5.85	Loss of integrity of information that should be protected
etc.	

Room M.811	
Confidentiality:	Normal
Integrity:	Normal
Availability:	High
T 1.4	Fire
T 1.5	Water
T 2.6	Unauthorised admission to rooms requiring protection
T 5.3	Unauthorised entry into a building
T 5.5	Vandalism
etc.	

4 Determination of additional threats

For the target objects under review there are, in some circumstances, additional isolated threats over and above those foreseen in the IT-Grundschutz Model. These must also be taken into consideration. As a general rule, the IT-Grundschutz Catalogues listed only those threats which

- Are conditional upon a particular technology, a specific product or a special application
- Can - in usual scenarios - only result in damage under very special conditions
- Require the attacker to have excellent expertise, opportunities and resources

These include, for example, deliberately eliminating a whole location using weapons or a technically complicated attack with the co-operation of an internal administrator.

For information security the *relevant threats* are those

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

When determining additional relevant threats, the protection requirement for the target object under review must be considered in terms of the three *basic parameters* for information security – *confidentiality, integrity* and *availability*:

1. If a target object has a *very high* protection requirement for a particular basic parameter, the threats that could adversely affect this basic parameter should be found first. In this security requirement category it should be assumed that there are relevant threats which are not contained in the IT-Grundschutz Catalogues.
2. Even if a target object has a *high* protection requirement for a particular basic parameter, the threats that could adversely affect this basic parameter should be found. In this security requirement category there may, in certain circumstances, be relevant threats which are not contained in the IT-Grundschutz Catalogues.
3. If the target object is categorised as having a *normal* security requirement in one specific basic parameter then the threats listed in the IT-Grundschutz Catalogues - and therefore also the recommended security measures - are generally adequate for this basic parameter.

Irrespective of the security requirement 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 Catalogues or if the target object is operated in a scenario (environment, application) which is not foreseen in the IT-Grundschutz Catalogues.

The following issues are to be considered when determining additional threats:

- Which potential force majeure events represent particular threats for the information domain?
- Which organisational failures must be avoided at all costs in order to guarantee information security?
- Which human errors adversely affect the security of information and applications?
- 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 institution 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 objects not located in the information domain being examined that represent special threats? Such external objects could be external applications, IT systems, or structural conditions, for example. The definition of the information domain being examined is used to specify the object to be examined for the security concept. However, this must not result in the neglection of threats which are located outside of the information domain being examined during the risk analysis.

For each target object under review the first step is to check whether any additional threats must be considered. Such sources of special threats may include

- The manufacturer's documentation
- Publications on vulnerabilities on the Internet and
- One’s own threat analyses.

When identifying additional threats it can also be worthwhile re-consulting the IT-Grundschutz Threat Catalogues T 1 to T 5 as sources. It may be that further relevant threats are listed there that were not previously taken into consideration because the respective modules may not, for example, be contained in the modelling process.

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 which threats may still be missing should therefore be performed. For this it is frequently advisable *to utilise external consulting services*..

Brainstorming involving all the relevant employees has proven effective in determining additional threats. IT security officers, project managers, administrators and users of the target object under review and possibly external experts, if appropriate, should be involved. The participants' objectives should be clearly formulated and the brainstorming time limited. Experience has shown that a period of 2 hours is an appropriate upper limit. An expert for information security should conduct the brainstorming session.

Example: (Excerpt)

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

Entire information domain	
T 2.U1	Inadequate synchronisation of active and backup system
	Because of the high availability requirements the components of the communication system to the customer exist in duplicate. If the backup components are not up to date, there is a risk that no working connection to the customer can be established.
T 5.70	Manipulation by family members or visitors
	This threat is contained in the IT-Grundschutz Catalogues and is referenced from module B 2.8 *Workplace at Home*. However, this module is not contained in the modelling of the current information domain. Nevertheless, threat T 5.70 must be taken into account because visitors are regularly shown through the firm’s premises. T 5.70 is therefore also included in the risk assessment.
etc.	

Switch N7	
Confidentiality:	normal
Integrity:	normal
Availability:	high
T 2.U2	Damage to information technology in production department
	The Client C4 and Switch N7 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.
etc.	

Client C4	
Confidentiality:	normal
Integrity:	high
Availability:	high
T 2.U2	Damage to information technology in production department
	Refer to Switch N7
T 4.U1	Incompatibility between production and communication software
	Client C4 is not only used to communicate with the customer, it is also used to operate other programs that support production. Incompatibility between these programs may result in crashes and loss of availability.
etc.	

5 Threat assessment

The next step works through the threat summary systematically. It checks whether the security measures already implemented or at least planned in the security concept provide adequate protection for each target object and threat. As a general rule, these will be standard security measures taken from the IT-Grundschutz Catalogues. The test is performed using the security concept and the following testing criteria:

- Completeness

  Do the standard security measures provide protection for all aspects of each threat? (Example: Was the back door to the building and on the emergency exits also considered?)

- Mechanism strength

  Do the protection mechanisms recommended in the standard security measures counteract each threat adequately? (Example: Are the specifications for the minimum key length adequate?)

- Reliability

  How difficult is it to circumvent the planned security mechanisms? (Example: How easy is it for users to gain entry to the server room and therefore circumvent the file access control?)

The result of the check is entered in the *OK* (*Y/N*) column in the threat summary for each individual threat.

OK=Y means that the security measures implemented or envisaged in the security concept provide *adequate protection* against the respective threat or that the threat is *not relevant* for the current risk analysis (for example, because another basic parameter is affected).

OK=N means that the security measures implemented or envisaged in the security concept do *not provide adequate protection* against the respective threat.

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

The risk assessment provides an overview as to which threats are adequately covered for the target objects under review by the measures contained in the IT-Grundschutz Catalogues (*OK=Y*), and as to where there may still be risks (*OK=N*). Dealing with these threats is discussed in the next section.

Example: (Excerpt)

A supplier carries out a threat assessment using the amended threat summary. The result is, e.g., that the IT-Grundschutz safeguards are not adequate for such threats as the following (*OK=N*):

Communication server S3		
Confidentiality: normal Integrity: high Availability: high		
T 1.2	Failure of the IT system	OK=N
	Reliable action must be taken to prevent Server S3 from failing. The IT-Grundschutz Catalogue measures are not adequate.	
T 5.85	Loss of integrity of information that should be protected	OK=N
	The order requirement information sent by the customer must not be tampered with. Otherwise, this could result in surplus production or supply shortages, thereby incurring high costs to the company.	

Communication server S3	
etc.	

Client C4		
Confidentiality: normal Integrity: high Availability: high		
T 1.2	Failure of the IT system	OK=N
	Special software whose installation is costly and time-consuming is used on Client C4 to communicate with the customer.	
T 2.U2	Damage to information technology in production department	OK=N
	The processing of information in automated production areas is only marginally dealt with in the IT-Grundschutz Catalogues.	
etc.		

6 Handling risks

6.1 Alternative methods for handling risks

In practice, the risk assessment usually identifies a number of threats which are not adequately counteracted by the measures contained in the IT-Grundschutz Catalogues. *Risks* for operating the information domain may arise from these *residual threats*.

Therefore, a decision on how to deal with the remaining threats has to be taken. In all cases management must be involved in this decision because there may under some circumstances be substantial risks or additional costs. The following alternatives exist for each threat in the threat summary that has been assigned *OK=N*.

A. *Risk reduction through additional security measures:* The residual threat is eliminated by working out and implementing one or more supplementary security measures that counteract the threat adequately. The following sources of information on supplementary IT security measures 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 the information Security Department’s committees
   - Other publications and services, for example, those offered on the Internet or by specialised companies
   - Experience gained within the institution or at co-operation partners

B. *Risk avoidance through restructuring:* The remaining threat is removed by restructuring the business process or information domain. The reasons for such changes may include:

   - All effective counteractions are too expensive, but the remaining threat cannot be accepted
   - Restructuring is appropriate for other reasons, such as reducing the costs
   - All effective counteractions would be accompanied by substantial restrictions to the functions or comfort of the system

C. *Risk acceptance:* The remaining threat and the risk arising from it are accepted. The reasons for such decisions may include:

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

D. *Risk transfer:* The risk ensuing from the remaining threat is transferred to another institution, by taking out an insurance policy, for example, or by outsourcing. The reasons for such decisions may include:

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

To prepare a well-founded decision as to which of the four handling options is chosen for each risk, a brainstorming session should be performed. During this session supplementary IT security measures (Alternative A) can be considered. The sources of information listed above should be used.

Notes:

IT-Grundschutz safeguards marked in the catalogues as additional (Z) can be used as starting points for further security safeguards in the context of a risk analysis. These safeguards are examples that go beyond the scope of IT-Grundschutz and which are commonly used in practical applications. Note though, that IT-Grundschutz safeguards marked as additional (Z) are not automatically binding, even when the security requirements are high. They also do not need to be integrated into a risk analysis.

In some cases it is possible to identify security measures that cover part – but not all – of the sub-aspects of a threat. Then the question of how to deal with the threat arises (Alternative A or C). The threat should be divided into two threats that can then be handled separately using Alternative A or C.

The existing security measures for the target object under review should also be considered. This may involve referring back to the results of the basic security check (see Section 4.5 of the IT-Grundschutz Methodology).

The hypothetical effort and cost of any security measures possibly required and information on existing security mechanisms are important decision-making aids.

- For Alternative A the supplementary security measures are added to the security concept. A clear reference to the corresponding, detailed description of the measures is sufficient.
- In general Alternative B results in restarting the IT security process for the affected parts of the information domain. In most cases this begins with the structure analysis. Naturally, this may involve referring back to the information and documentation previously compiled.
- For Alternative C the resulting risk must be made transparent. The decision is taken by management and clearly documented.
- For Alternative D the appropriate form of contract is one of the most important aspects. Sound legal advice should be taken on this, particularly in the case of outsourcing schemes. The decision is taken by management and clearly documented.

Important: Where no sufficiently effective countermeasures are specified in the IT-Grundschutz Catalogues for certain threats, the manner in which the latter are handled can be critical for the overall IT system risk in the information domain under examination. Due consideration should be given to using external consulting services in these matters.

6.2 Risks under examination

During the risk analysis, threats may be identified under some circumstances that lead to risks which may be acceptable now, but which will probably increase in the future. This means that it may be necessary to take action during further development. In such cases, it is appropriate and common to prepare and create supplementary security safeguards in advance. These safeguards can then be put in to operation as soon as the risks become unacceptable. These supplementary security safeguards are to be documented and marked separately. In the documentation of the risk analysis, the corresponding threats are initially marked with a "C", and the risks resulting from them are examined. As soon as the risks become unacceptable, the supplementary security safeguards marked are checked, updated if necessary, and added to the security concept. The handling for the corresponding threats is changed to "A" in the documentation of the risk analysis. The handling could also be set to "B" or "D" as an alternative in this case as well.

After a decision on which of the handling options described is to be selected for each remaining threat in the threat summary, it is possible to produce the security concept for the information domain under review.

Example: (Excerpt)

The following decisions are taken for the threats identified in Section 0 as *OK=N*:

Communication server S3	
Confidentiality:	normal
Integrity:	high
Availability:	high
T 1.2	Failure of the IT system
"A"	Supplementary IT security measure:
S 6.U1	Provision of a complete replacement system for communicating with the customer A complete replacement system for communicating with the customer will be provided. This covers all the technical modules including communication links. The replacement system will be located in Room E.3. It must be ensured that the replacement system has the same configuration as the production system at all times and can be used within 30 minutes. The communication with the customer takes place over a dial-up connection. The whole replacement system including dial-up connection is tested at least once a quarter and whenever the configuration is changed.
T 5.85	Loss of integrity of information that should be protected
"C"	Risk acceptance: Although the risk is minimised to some extent by the safety mechanisms built into the transmission and IT systems, there could be further security incidents leading to the adulteration of order requirement information and thereby incurring high costs for the company. This remaining risk is accepted and the responsibility is taken by management, because all effective counteractions are uneconomic.
etc.	

Client C4	
Confidentiality:	Normal
Integrity:	High
Availability:	High
T 1.2	Failure of the IT system
"A"	Supplementary IT security measure:
S 6.U1	Provision of a complete replacement system for communicating with the customer **Note**: Refer to Communication server S3
T 2.U2	Damage to information technology in production department

Client C4	
"A"	Supplementary IT security measure:
S 1.U1	Use of a specially protected industrial PC in the production area The greatest threats to Client C4 in the production area result from air pollution, water splashes and vibrations. Instead of a commercial PC, an industrial PC that is specially protected from physical threats will be used. The industrial PC must meet the following requirements: - Suitable for installation in a standard 19 inch slot - Integrated or fold-out display - Easily exchangeable air filter - Protection against splashed water in accordance with protection type IP 54 - Protection against vibration to at least 0.2 g at 0-500 Hz
etc.	

7 Consolidation of the security concept

If additional security measures must be added when handling the remaining threats, the security concept must subsequently be consolidated. Specifically, this means checking the security measures for each target object using the following criteria:

Suitability of security measures 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 measures

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

User friendliness of security measures

- Are the measures tolerant towards user and operating errors?
- Are the measures transparent for users?
- Is it clear to the users if a measure is omitted?
- Is it too easy for users to circumvent the measure?

Appropriateness of security safeguards

- Are the measures 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:

1. Inappropriate security measures should be rejected and after a detailed analysis replaced by effective measures.
2. Contradictions or inconsistencies in the security measures should be resolved and replaced by homogenous mechanisms that are co-ordinated with each other.
3. Security measures that are not accepted by users have no effect. Practical solutions that restrict or hinder users as little as possible should be found.
4. Security measures that are too difficult or costly should either be re-worked or rejected and replaced by appropriate protective measures. On the other hand, measures that are too weak endanger IT security. They should also be reworked or replaced.

It can be eminently advisable to adopt further practices for improving information security, such as penetration tests. These aim to simulate the behaviour of a deliberate perpetrator (insider or outsider). The results may in turn produce changes to the existing security concept.

Example: (Excerpt)

When consolidating the security concept for the supplier company, the following issues were found:

- The relevant measures from the IT-Grundschutz Catalogues must also be taken for the replacement system called for in S 6.U1. The differences to the production system are only with regard to installation location and WAN connection. Therefore, the replacement system must be integrated into the IT-Grundschutz model.
- Measure S 6.53 *Redundant arrangement of network components* planned on the basis of the IT-Grundschutz is made more specific for Switch N7 by Measure S 6.U1. After implementing S 6.U1, S 6.53 has also been implemented for target object N7. Measure S 6.53 can therefore be deleted from the security concept for Switch N7.
- Two years ago it was decided that Measure S 5.68 *Use of encryption procedure for network communication* 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 adapted to the current requirements.
- The supplementary IT security measure S 1.U1 considers the basic infrastructure specific to Client C4. 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 implementation of Measure S 1.U1 as an opportunity to develop a policy governing the safe operation of information technology in the production area.
- etc.

8 Feedback to the security process

Once the security concept has been consolidated, the security process, as specified in the IT-Grundschutz Methodology, can be resumed. Therefore, the adjusted security concept becomes the basis for the following work steps:

- *Basic security check* (Section 4.5 of the IT-Grundschutz Methodology). A basic security check has already been performed as part of the preliminaries in accordance with the measures provided under the IT-Grundschutz model. Since the risk analysis generally produces changes in the security concept, the subsequent implementation status of additional and altered measures must be checked. If necessary, outdated results should be updated.
- *Implementing the security concept* (Section 5 of the IT-Grundschutz Methodology). The security measures planned in the security concept for individual target objects must be implemented in practice for them to be effective. Among other things, this includes estimating costs and expenses and deciding on the order of implementation.
- *Reviewing the information security process on all levels* (Section 6.1 of the IT-Grundschutz Methodology). To maintain and continually improve the information security, the implementation of the security safeguards and the suitability of the security strategy must be checked on a regular basis, among other things. The results of the checks are incorporated in the updates of the security process.
- *Information flow in the information security process* (section 6.2 der IT-Grundschutz-Vorgehensweise). To make the security process understandable, the security process must be documented at all levels. This includes in particular clear rules for reporting paths and the information flows. Management must be kept duly informed by the security organisation about results of reviews, IT security incidents, the status of the IT security process and, where applicable, about any further status of information security. This process of passing on information should highlight any problems, positive achievements and potential improvements.
- *ISO 27001 Certification on the basis of IT-Grundschutz* (Section 7 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 internally and externally. To this end the BSI has established appropriate mechanisms by way of IT-Grundschutz Attestation and " the auditor attestations and the ISO 27001 Certification in compliance with IT-Grundschutz".
- *Transfer to GSTOOL* (Refer to *http://www.bsi.bund.de/gstool*). Where the security management is supported by GSTOOL or other software, the results of the risk analysis should, as far as possible, be incorporated therein. In the case of GSTOOL this applies in particular to new or revised security measures which are not contained in the IT-Grundschutz Catalogues in this form.