Verein Hanseatischer Transportversicherer e.V.

IT-Grundschutz Profile for Shipping Companies

Minimum Protection for Shore Operations

Bremen, 18/12/2018

Change History

Version	Date	Name	Description
1.0	16/10/2018	BSI	Preparation of Working Draft 1.0
1.0	30/11/2018	BSI, VHT, afEfa Verwaltungsgesellschaft mbH	Summary of findings from the workshops
1.0	18/12/2018	VHT	Finalisation

TABLE OF CONTENTS

1 Preface

In November 2017, the VHT – Verein Hanseatischer Transportversicherer e.V. – organised its annual loss prevention seminar for its members and clients. The topic this time was 'Cyber risks in shipping'. The issue was very actual, because five months earlier the maritime industry had also been hit by the 'NotPetya' blackmail Trojan.

The feedback from the participants was so good that we decided to continue with the topic. Research soon made it clear that while a plethora of cyber-security vendors exists, there were no bespoke security systems specifically available for ship owners and ships – or, if there were, only isolated applications.

During our search, we inevitably came across the Federal Office for Information Security (BSI) in Bonn. We described our ideas and plans to them, and, after just four months, were able to start working together in the form of a kick-off workshop.

During the first workshop, the decision was made to address protecting shore operations first. The preparations for protecting ship operations will be presented in another series of workshops starting in January 2019.

In just three meetings, we succeeded in creating the "IT-Grundschutz profile for shipping companies. Minimum protection for shore operations" (for short: “Grundschutz profile for shipping companies – Shore operations”).

The “Grundschutz profile for shipping companies – Shore operations” provides you with a useful tool that not only improves your cyber security, but also largely covers the requirements of data protection (BDSG and GDPR) and ISO 9001 certification.

Keep in mind that, according to the International Maritime Organization (IMO), a cyber-security concept of this nature must be in place by January 1, 2021!

Together with the BSI, we at VHT would like to offer you further support and invite you, as a shipping company, to the next free series of workshops on, "Grundschutz profile for shipping companies – Ships".

Acknowledgements

At this point I would like to thank everyone involved. In particular, I would like to express my thanks to Ms Frauke Greven and Mr Birger Klein from the BSI, who quickly succeeded in plumbing the ins and outs of the shipping sector and guided us to our destination with a great deal of fun and humour.

I would also like to thank Mr Kersten Gevers from the company afEfa Verwaltungsgesellschaft mbH, who, in the aftermath of the seminars, looked back on them and reappraised the corresponding stages and summarised them.

Last but not least, I would like to express my gratitude to my colleague, Ms Birte Stützle, who arranged the organisation and catering and created a pleasant working atmosphere for everyone involved.

My thanks go out to you all!

Uwe Reder, VHT

2 Introduction

Shipping companies are obliged to take technical and organisational measures in order to adequately protect their IT systems and business processes. These obligations arise, by way of example, from data protection needs (e.g. EU General Data Protection Regulation (EU GDPR) and the German Federal Data Protection Act 2018 (BDSG)) and, in future, from the requirements of the International Maritime Organization (IMO). In addition, the substantial investments that shipping companies make in their IT equipment are to be protected using appropriate safeguards. With regard to the principles of economy, the profile described here includes the minimum requirements for preventing widespread material and non-material damage (e.g. damage to reputation or loss of trust) that could arise for a shipping company from a breach of confidentiality, manipulation of data or unavailability of the IT infrastructure.

As part of its involvement in the Alliance for Cyber Security, an initiative of the Federal Office for Information Security (BSI), VHT has initiated a process in cooperation with the BSI that makes it easier for shipping companies to adapt their security concept to their individual framework conditions based on IT-Grundschutz. The IT-Grundschutz from the BSI represents a tried-and-tested methodology for increasing the level of information security in organisations of all sizes.

This IT-Grundschutz profile has been compiled to make it easier for you to get started with the IT security process. An IT-Grundschutz profile represents a model security concept that serves as a template for organisations with comparable framework conditions. Steps to be taken for IT-Grundschutz are generalised in this example, to ultimately enable all interested shipping companies to use the template to increase information security in their own organisations. This saves a lot of work and time.

Based on two business processes that are considered to be relevant, this white paper on "IT-Grundschutz profile for shipping companies – Minimum protection for shore operations" includes:

- A list of relevant target objects (applications, IT systems and premises) to be protected.
- An assignment of matching IT-Grundschutz modules with requirements and implementation guidance and
- Recommendations for the implementation sequence.

The following provide central support for implementation in the organisation:

1. A "Map" for the management team as a basis for making decisions and an "Implementation Roadmap" for IT professionals.

2. Recommendations for the focussed use of the comprehensive requirements and implementation guidance from the IT-Grundschutz of the BSI.

3 Formal aspects

Title:	"IT-Grundschutz profile for shipping companies – Minimum protection for shore operations
Authors:	See Sec. 5, "List of authors"
Publisher:	Verein Hanseatischer Transportversicherer e.V. (VHT)
Registration number:	To be issued by the BSI after successful completion of the registration process
Version status:	Published on 18/12/2018, Version 1.0, finalised in December 2018
Revision cycle:	This white paper should be reviewed every three years to verify its actuality.
Confidentiality:	This version of the white paper is openly accessible. A classified version will also exist, which will only be accessible to users who were or are involved in preparing the further version. It is envisaged that the TLP (Traffic Light Protocol) classification will be "Amber".

4 Disclaimer

This white paper has been prepared with the utmost care but makes no claim to be complete or correct. The contributors to this white paper have no control over its further use by individual users and therefore cannot be held liable for the impact on the legal position of the parties.

5 Copyright

6 List of authors

The participants in the workshop series developed by the BSI, "IT-Grundschutz profiles for shipping companies", were involved in the preparation of this white paper. The workshops were organised by VHT, with the moderation being taken over by the BSI. The participants are listed in the following table in alphabetical order.

Name	**Organisation**
Silke Angermann	ERGO Versicherung AG
Eckhard Bartkowski	SLOMAN NEPTUN Schiffahrts-Aktiengesellschaft
Jürgen Berentzen	WESSELS Reederei GmbH & Co. KG
Wilko Cramer	Aktiengesellschaft Reederei Norden-Frisia
Cpt. Peter Dopp	Navo Mare GmbH & Co. KG
Dipl. Ing. Kersten Gevers (graduate engineer)	afEfa Verwaltungsgesellschaft mbH
Torsten Gevers	Reederei Gerdes Gruppe
Andreas Held	RIGEL Schiffahrts GmbH & Co. KG
Louis Ravens	Lampe & Schwartze KG
Uwe Reder	Verein Hanseatischer Transportversicherer e.V.
Jan Ruhnau	Bremer Bereederungsgesellschaft mbH & Co. KG
Mathias Waack	DAL Deutsche Afrika-Linien GmbH & Co. KG; John T. Essberger GmbH & Co. KG
Udo Wienstroer	EMDER SCHLEPP-BETRIEB GMBH

7 Management summary

7.1 Target audience

This IT-Grundschutz profile is aimed at shipping companies that want to ensure information security in shore operations.

It is specifically intended for managers, IT administrators and QA managers who are responsible for implementing and maintaining information security.

7.2 Purpose

This IT-Grundschutz profile defines the minimum protection requirements for shipping companies on shore in the business processes 'Accounting' and 'Technical Management'. The profile assists in taking the first steps in information security and getting started with identifying the most serious vulnerabilities in the aforementioned processes, and also provides support in determining further protection needs and risk analysis.

In order to define the minimum protection requirement for the entire shipping company on shore, all other business processes at the shipping company need to be included in accordance with the strategy for this IT-Grundschutz profile.

7.3 Tasks at management level

The authors recommend that the management level at shipping companies use this profile as the basis for their information security concept for shore operations. That said, however, this IT-Grundschutz profile makes exclusive reference to the business processes "Accounting" and "Technical Management" and does not make reference to the entire organisation at a shipping company. All other relevant business processes would need to be recorded and documented accordingly for them to be covered. This would then make it possible to determine the minimum protection requirement for shore operations and select appropriate protective measures.

The authors recommend that shipping companies who use third parties to operate parts of their technical infrastructure, for instance, use this profile as a basis for selecting the respective service providers. The requirements formulated here should be included in the terms of contract.

8 Specification of the scope

8.1 Target audience

This IT-Grundschutz profile is aimed at shipping companies that want to ensure information security in shore operations.

8.2 Protection needs

This IT-Grundschutz profile defines a level of protection that, in parts, lies above the Standard Protection of the IT-Grundschutz.

As a rule, large amounts of personal data are processed, and the confidentiality of this data is given high priority within the framework of the business process 'Accounting'. In addition, an increased need for protection usually exists regarding the availability of the services offered. For these areas, the protection needs is therefore assumed to be "high" in terms of confidentiality and integrity.

As a rule, very large volumes of technical and essentially key data is transmitted, captured and processed within the framework of the business process 'Technical Management'. A very high protection needs exists here regarding the implementation of the "PMS software" module. Depending on the state of the information technology used in the organisation, the business process "Preventive Maintenance PMS" can lead to serious impairment in fulfilment of the task, as well as a loss of integrity causing potentially serious damage, without the availability of the application and/or the data.

The protection needs determined here need to be taken into account when using the IT-Grundschutz profile.

8.3 IT-Grundschutz procedure

The requirements listed in this IT-Grundschutz profile are recommendations to shipping companies for implementing information security in shore operations. At a minimum, they cover the "Standard Protection" requirements of BSI Standard 200-2, and, in some cases, requirements relating to high or very high protection needs also need to be implemented.

8.4 Coverage strategy

Using the IT-Grundschutz profile for shipping companies achieves the standard level of protection and in some cases the "high" and "very high" level of protection for the IT infrastructure and the business processes addressed.

8.5 ISO 27001 compatibility

Implementation of the IT-Grundschutz approach "Standard Protection" makes it compatible with ISO 27001.

8.6 Framework conditions

The information security requirements described in this profile take into account the requirements of the EU General Data Protection Regulation (EU GDPR), the German Federal Data Protection Act (BDSG 2018) and the future requirements of the International Maritime Organization (IMO).

8.7 Obligation to fulfil

It follows from the standards mentioned in Sec. 8.6 that shipping companies are obliged to ensure information security. Information security can be ensured with the help of this IT-Grundschutz profile.

9 Specification of the information domain

9.1 Components in the information domain

The information domain for a shipping company's shore operations includes all processes, applications, IT systems and rooms and facilities required for executing the entire process at a shipping company.

This IT-Grundschutz profile is limited to the business processes 'Accounting' and 'Technical Management' and takes into account the applications, IT systems and rooms and facilities linked to them.

9.2 Objects not taken into account

This IT-Grundschutz profile does not take account of all the remaining processes required for executing the overall process in shore operations at a shipping company. The authors are convinced that the two business processes selected, 'Accounting' and 'Technical Management', are sufficiently representative of all business processes not accounted for and that a shipping company can use this IT-Grundschutz profile highly effectively as a basis for the development and continuation of an individual information security management system. In addition to the two aforementioned business processes, the following operational application areas were covered in essence within the scope of the structural analysis: chartering, operations, human resources, QHSE (Quality, Health, Safety and Environment), insurance management, interface communication, purchasing and marketing.

Furthermore, information security on board a ship managed by the shipping company has been expressly disregarded. The opinion of the authors is that information security aboard a ship should be the subject of a separate IT-Grundschutz profile. When creating such a profile, it needs to be remembered that the processes, applications, IT systems and rooms and facilities aboard a ship are largely covered by international regulations (e.g. model specifications, equipment regulations).

9.3 Link to other IT-Grundschutz profiles

There are no references to other IT-Grundschutz profiles at this time.

10 Reference architecture

The reference architecture (also referred to as the 'object under investigation') specifies which objects the requirements of the IT-Grundschutz in terms of this IT-Grundschutz profile need to be applied to.

These include:

- Business processes
- Applications (software programmes)
- Existing IT systems (incl. clients, servers, network coupling elements, mobile devices) as well as networks, communication devices and external interfaces deployed
- Spatial conditions/infrastructure (properties, buildings, rooms).

10.1 Object under investigation

10.1.1 Business processes

The **business process 'Accounting'** comprises the following sub-processes:

- Accounting – Shore (shipping company)
- Accounting – Ocean (ocean carrier)
- Accounting – Crew/Shore Staff (ship’s management/personnel service companies)
- Organisation – Payment Processes
- Payment Transactions
- Reporting
- Accounting/Taxes/Auditing.

The **business process 'Technical Management'** comprises the following sub-processes:

- Planning/Performance of class renewal and shipyard stopover
- Ship Inspections/Visits
- Corrective Action
- Maintenance/Planned Maintenance
- Organisation – Repairs and service.

10.1.2 Applications

- APP.1.1 Office Products
- APP.1.2 Web Browser
- APP.3.3 File Server
- APP.5.2 Microsoft Exchange and Outlook

10.1.3 IT systems

- SYS.1.1 General Server
- SYS.1.5 Virtualisation
- SYS.1.8 Storage Solutions
- SYS.2.1 General Client
- SYS.3.1 Laptops
- SYS.3.2.1 General Smartphones and Tablets
- SYS.3.2.2 Mobile Device Management (MDM)
- SYS.3.4 Mobile Data Carriers
- SYS.4.1 Printers, Copiers and All-in-One Devices

10.1.4 Networks and communication

- NET.1.1 Network Architecture and Design
- NET.1.2 Network Management
- NET.2.1 WLAN Operation
- NET.3.1 Routers and Switches
- NET.3.2 Firewall
- NET.3.3 VPN

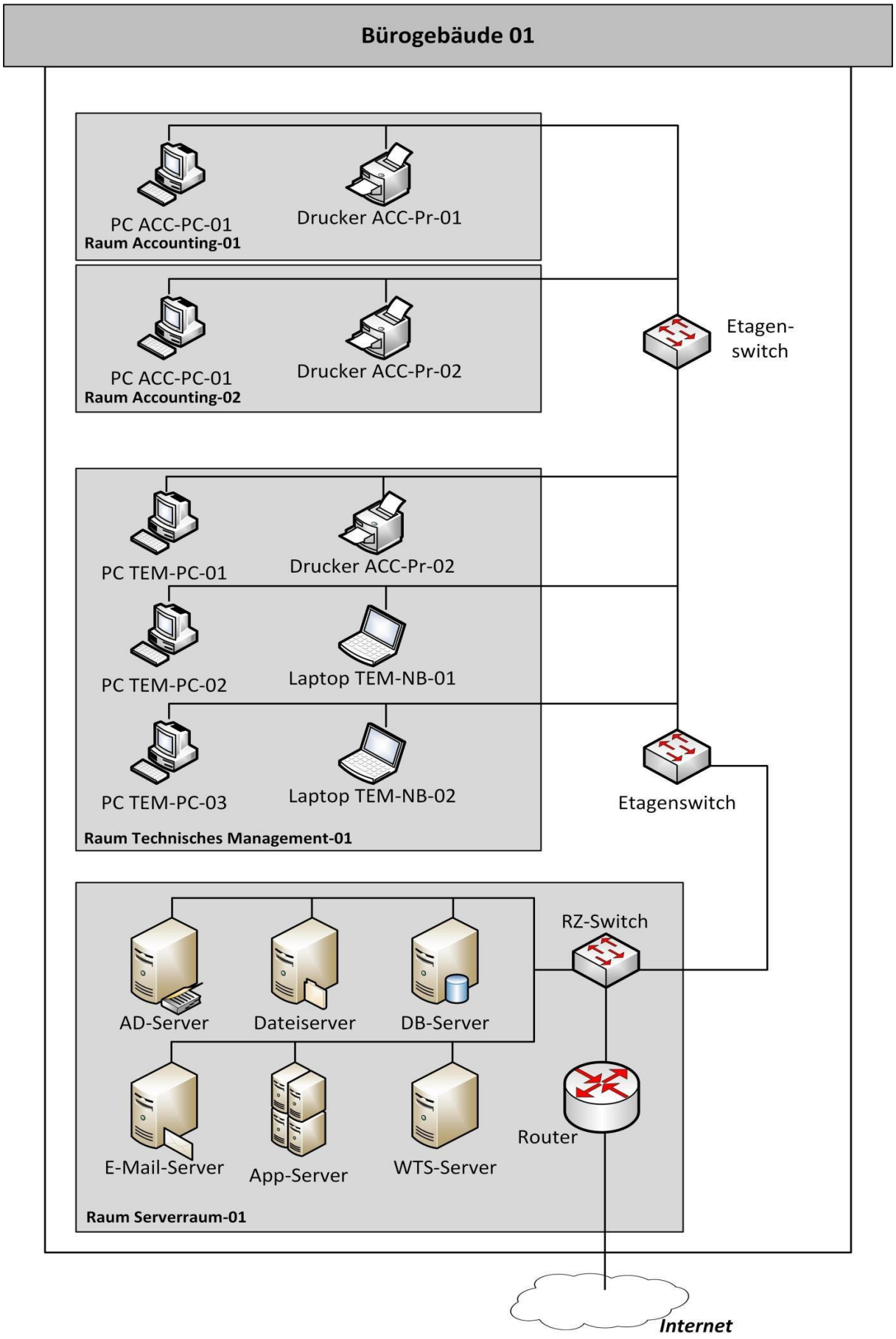
10.1.5 Infrastructure

- INF.1 General Building
- INF.2 Data Center/Server Room
- INF.3 Cabling
- INF.4 IT Cabling
- INF.7 Office / Local Workspace
- INF.8 Home Workplace
- INF.9 Mobile Workplace

10.2 Addressing differences

If the information domain to be protected deviates from the reference architecture, then additional or non-existing objects need to be documented. Suitable modules from the IT-Grundschutz Compendium are to be assigned to these. The requirements derived from the modules need to be adapted depending on the desired protection level.

10.3 Network plan



11 Requirements to be fulfilled and measures to be implemented

Suitable IT-Grundschutz modules can be selected based on the reference architecture. These contain explanations on the risk exposure and security requirements, along with further information.

The modules from the IT-Grundschutz Compendium listed in this IT-Grundschutz profile generally suffice to achieve the desired security level. Operational environments or components that deviate from the IT-Grundschutz profile require the use of other components in some circumstances. A review is therefore required within the context of using the IT-Grundschutz profile.

Tip for the management team:
Each IT-Grundschutz module contains information of the exposure to risk that describes the risks of failing to implement the recommended security requirements.

Additional implementation information with detailed descriptions of suitable security measures that can be used as a basis for security concepts exists for many modules.

11.1 Everything at a glance – work aids: “Map”

The map presents an overview of all the key findings from the structural analysis and the modelling (selection of suitable IT-Grundschutz modules) – beginning with each "key" business process in the reference architecture (applications, IT systems and rooms and facilities), the respective protection needs and the assignment of the IT-Grundschutz modules, including recommendations for the implementation sequence. In cases where it is not possible to allocate existing modules, it becomes clear that an in-house risk analysis and possibly organisational and/or industry-specific solutions are required.

The maps offer virtually "everything at a glance" and thus open up access to the bespoke IT security process. This can serve both as a basis for decision-making for the company management and as an "implementation roadmap" for IT professionals.

The maps of the two business processes discussed here can be found in the Annex:

- Business process – 'Accounting' (14.1)
- Business process – 'Technical Management' (14.2)

Information on using the map:
The map should be read column-by-column rather than row-by-row. Column 1 names the business processes relevant to shipping companies. Column 2 details the business processes using typical tasks in this area. The outcome of this are the applications needed to perform the tasks (Column 3). These applications conclude with the corresponding IT systems (Column 4) located in certain rooms and facilities in the operation (Column 5).

The **symbols "!" and "!!"** make it clear that the object referred to is of particular importance to the performance of the tasks in the respective business process. For example, they could indicate to senior management to prioritise efforts to protect this target object:

- ➔ No exclamation mark = Normal – The business process or specialist task can be carried out by other means (e.g. manually) with a tolerable amount of additional effort.
- ➔ One exclamation mark = High – The business process or specialist task can only be carried out by other means with a clear amount of additional effort.
- ➔ Two exclamation marks = Very High – The business process or specialist task cannot be carried out at all without the application.

Marking with one or two **security shields** refers to a special need for protection. Since the protection needs is not usually quantifiable, IT-Grundschutz is limited to a qualitative statement by dividing the protection needs into three categories:

Category of protection needs	
"Normal" (not marked)	The effects of damage are limited and manageable.
"High" (one security shield)	The effects of damage can be considerable.
"Very High" (two security shields)	The effects of damage can reach a catastrophic extent that represents an existential threat.

The **white shields** refer to appropriate IT-Grundschutz modules to be used on the respective target object. A module can play a role in several business processes. Implementation of the respective security requirements can result in synergies, because the measures implemented for a prioritised business process immediately radiate out and have an effect on other business processes.

If the applications, IT systems, rooms and facilities are marked with a **white asterisk (*)**, this shows that further steps are required to achieve the desired security level. The individual meaning of the various markings are:

***** The modules listed here from the IT-Grundschutz Compendium do not suffice alone to achieve the desired security level. Further requirements and implementation information need to be developed individually.

****** Currently, the IT-Grundschutz Compendium does not contain a module for this. Requirements and implementation information need to be developed individually.

If applications, IT systems, and rooms and facilities do not have an asterisk, this means that the modules listed in the IT-Grundschutz Compendium suffice for achieving the desired security level.

11.2 Overview I: General modules (relevant to the organisation as a whole)

Tip for the implementation sequence:

The following modules have notes added to the processing sequence:

- R1: These modules need to implemented as a priority since they form the basis for an effective security process.
- R2: These modules should be implemented next, since they are required as key components in the sustainable security information network.
- R3: These components are also needed to achieve the desired security level and have to be implemented, but we recommend considering them after the other components.

11.2.1 ISMS.1 Security Management (R1)

11.2.2 ORP: Organisation and personnel

ORP.1 Organisation (R1)
ORP.2 Personnel (R1)
ORP.3 Awareness and Training (R1)
ORP.4 Identity and Access Management (R1)
ORP.5 Compliance Management (R3)

11.2.3 CON: Conception and approaches

CON.1 Crypto Concept (R3)
CON.2 Data Protection (R2)
CON.3 Backup Concept (R1)
CON.4 Selection and Use of Standard Software
CON.5 Development and Use of General Applications (R3)
CON.6 Deleting and Destroying Data (R1)
CON.7 Information Security on Trips Abroad (R3)

11.2.4 OPS: Operation

OPS.1.1.2 Proper IT Administration (R1, if the shipping company performs IT administration in-house)
OPS.1.1.3 Patch and Change Management (R1)
OPS.1.1.4 Protection Against Malware (R1)
OPS.1.1.5 Logging (R1)
OPS.2.2 Cloud Usage
OPS.2.4 Remote Maintenance (R3)

11.2.5 DER: Detection and reaction

DER.1 Detection of Security Incidents (R2)
DER.2.1 Handling Security Incidents (R2)
DER.2.2 Provisioning for IT forensics (R3)
DER.3.1 Audits and Revisions (R3)
DER.4 Business Continuity Management (R3)

11.3 Overview II: Business-relevant modules

11.3.1 OPS: Operation

OPS.1.2.4 Teleworking (R3)
[OPS.3.1 Outsourcing for Service Providers (for contracted ship management) (R3)]

11.3.2 APP: Applications

APP.1.1 Office Products (R2)
APP.1.2 Web Browser (R2)
APP.1.4 Mobile Applications (Apps)
APP.3.1 Web Applications (R2)

APP.3.3 File Server (R2)
APP.5.1 General Groupware (R2)
APP.5.2 Microsoft Exchange and Outlook (R2)

11.3.3 SYS: IT Systems

SYS.1.1 General Servers (R2)
SYS.1.2.2 Windows Servers 2012
SYS.1.5 Virtualisation (R2)
SYS.1.8 Storage Solutions (R2)
SYS.2.1 General Clients (R2)
SYS.2.2.2 Windows 8.1 Clients
SYS.2.2 .3 Windows 10 Clients
SYS.3.1 Laptops (R2)
SYS.3.2.1 General Smartphones and Tablets (R2)
SYS.3.2.2 Mobile Device Management (MDM) (R2)
SYS.3.2.3 iOS (for Enterprise)
SYS.3.2.4 Android
SYS.3.3 Mobile
/Telephones
SYS.3.4 Mobile Data Media (R2)
SYS.4.1 Printers, Copiers and All-in-One Devices (R2)
SYS.4.4 General IoT Device

11.3.4 NET: Networks and communication

NET.1.1 Network Architecture and Design
(R2)
NET.1.2 Network Management (R2)
NET.2.1 WLAN Operation (R2)
NET.3.1 Routers and Switches
(R2)
NET.3.2 Firewalls (R2)
NET.3.3 VPN (R2)
NET.4.1
Telecommunication
systemsNET.4.2
VoIP NET.4.3 Fax
Machine and Fax
Servers

11.3.5 INF: Infrastructure

INF.1 General Building (R2)
INF.2 Data Center/Server Room (R2)
INF.3 Cabling (R2)
INF.4 IT Cabling (R2)
INF.7 Office / Local Workplace (R2)
INF.8 Home Workplace (R2)
INF.9 Mobile Workplace (R2)

12 Residual risk assessment/risk response

The Basic and Standard Requirements of the IT-Grundschutz modules have been defined so that suitable measures for normal protection needs and typical information domains and application scenarios offer appropriate and sufficient protection. For this purpose, a preliminary investigation was carried out to identify the threats which the issues addressed in the modules are usually exposed to and how the risks that result from them can be appropriately countered. As a rule, users of the IT-Grundschutz profile no longer need to spend a great deal of time and effort investigating the security measures required for the vast majority of the information domain selected.
An additional need for analysis only exists in the following three cases:

- A target object has a high or very high protection needs in at least one of the three basic factors of confidentiality, integrity and availability.
- The IT-Grundschutz Compendium does not contain a sufficiently adequate module for a target object.
- Although there is a suitable module, the deployment environment for the target object is atypical for IT-Grundschutz.

Directions for performing a risk analysis can be found in Section 13.

13 Directions for use

I. Directions on how to determine protection needs

At a minimum, the requirements listed in this IT-Grundschutz profile cover the "standard protection" requirements of BSI Standard 200-2. Requirements relating to high protection needs might also need to be implemented.
A "Normal" security level needs to be assumed for the underlying business processes, and individual determination of the protection needs is therefore strongly recommended.

Information on the category of protection needs
Since the protection needs is not usually quantifiable, IT-Grundschutz is limited to a qualitative statement by dividing the protection needs into three categories:

Category of protection needs	
"Normal"	The effects of damage are limited and manageable.
"High"	The effects of damage can be considerable.
"Very High"	The effects of damage can reach a catastrophic extent that represents an existential threat.

Protection needs category: "Normal"	
1. Breaches of laws/regulations/ contracts	• Breaches of regulations and laws with minor consequences • Minor breaches of contract with low maximum penalties
2. Impairment in the right of informational self-determination	• This concerns personal data, the processing of which can compromise the data subject in his social standing or economic circumstances.
3. Impairment in personal integrity	• An impairment appears not possible.
4. Impairment in fulfilling a task	• The impairment would be considered tolerable by data subjects. • The maximum tolerable downtime lies between 24 and 72 hours.
5. Negative interior or exterior effect	• A slight or solely internal effect on reputation or trust is to be expected.
6. Financial impact	• The financial damage remains tolerable for the organisation.

Table 1: Protection needs category: "Normal"

Protection needs category: "High"	
1. Breaches of laws/regulations/ contracts	• Breaches of regulations and laws with significant consequences • Breaches of contract with high penalties
2. Impairment in the right of informational self-determination	• This concerns personal data, the processing of which can compromise the data subject in his social standing or economic circumstances.
3. Impairment in personal integrity	• Impairment in personal integrity cannot be completely ruled out.
4. Impairment in fulfilling a function	• The impairment would be considered intolerable by data subjects. • The maximum tolerable downtime lies between one and 24 hours.
5. Negative interior or exterior effect	• A broad effect on reputation or trust is to be expected.
6. Financial impact	• The damage causes considerable financial losses but is not existential in its threat.

Table 2: Protection needs category: "High"

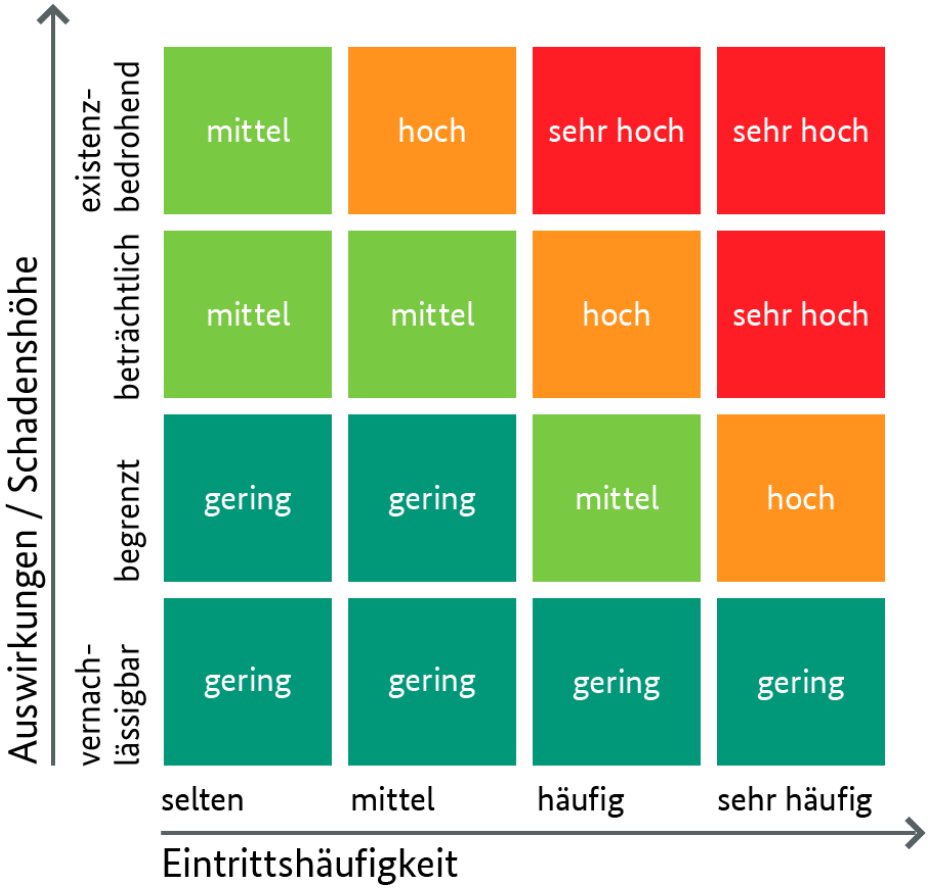
Protection needs category: "Very High"	
• Breaches of laws/regulations /contracts	• Fundamental breach of regulations and laws • Breaches of contract where the resulting losses due to liability are ruinous
• Impairment in the informational right of self-determination	• This concerns personal data, the processing of which poses a risk to the life and limb or the personal freedom of the data subject.
• Impairment in personal integrity	• Serious impairment in personal integrity is possible. • Risk to life and limb
• Impairment in fulfilling a function	• The impairment would be considered intolerable by all data subjects. • The maximum tolerable downtime is less than one hour.
• Negative interior or exterior effect	• A nationwide impairment in trust or reputation is conceivable, possibly even of a nature that threatens the existence of the organisation.
• Financial impact	• The financial damage poses a threat to the existence of the organisation.

Table 3: Protection needs category: "Very High"

II. Directions for performing a risk analysis

A risk analysis represents the basic procedure for investigating security threats and their effects. BSI Standard 200-3: "*Risk Management"* offers an efficient methodology for this. For the specific procedure and a detailed description, we therefore refer you to BSI Standard 200-3 at this point. Below is a short list of the steps to be performed in a risk analysis:

- **Compile target objects**
  The prerequisite for performing risk analyses in the context of standard protection is that the structural analysis includes the target objects in the information domain for which protection needs have been identified, and, where possible, that suitable IT-Grundschutz modules have been assigned to them during the modelling process. A risk analysis needs be performed on those target objects with a high or very high protection needs in at least one of the three basic values of confidentiality, integrity and availability, or for which no suitable IT-Grundschutz module exists, or which operate in deployment scenarios which are atypical for IT-Grundschutz.
- **Prepare threat summary**
  The first step in a risk analysis is to identify the risks to which an object or environment is exposed. The threats to which the object or environment are subject are to be described first for this purpose. The BSI has compiled a list of elementary threats to this end.
- **Complete threat summary**
  Although the process of compiling the elementary threats takes into account a variety of threats to which information and information technology are exposed, it cannot be ruled out that further threats will need to be considered. This is especially true if no suitable module exists for a target object, or if the object is operated in atypical deployment scenarios. Following the first sub-step, you should therefore check whether other threats need to be investigated in addition to the relevant elementary threats.
- **Estimate frequency and impact**
  The level of risk results from the frequency of a threat and the threat of damage. A risk is greater the more frequently a threat occurs. Conversely, the threat decreases the lower the possible damage. In principle, both factors can be determined both quantitatively, i.e. with precise numerical values, and qualitatively, i.e. with the aid of categories to describe the order of magnitude.
- **Evaluate the risks**
  After assessing the frequency of occurrence and the damage impact of a threat, you can assess the risk that results from both factors. Not using too large a number of categories is also appropriate here, with three to five categories being common. Often only two categories are used. BSI Standard 200-3 contains an example that contains four levels that you can adapt to the circumstances and needs of your organisation.



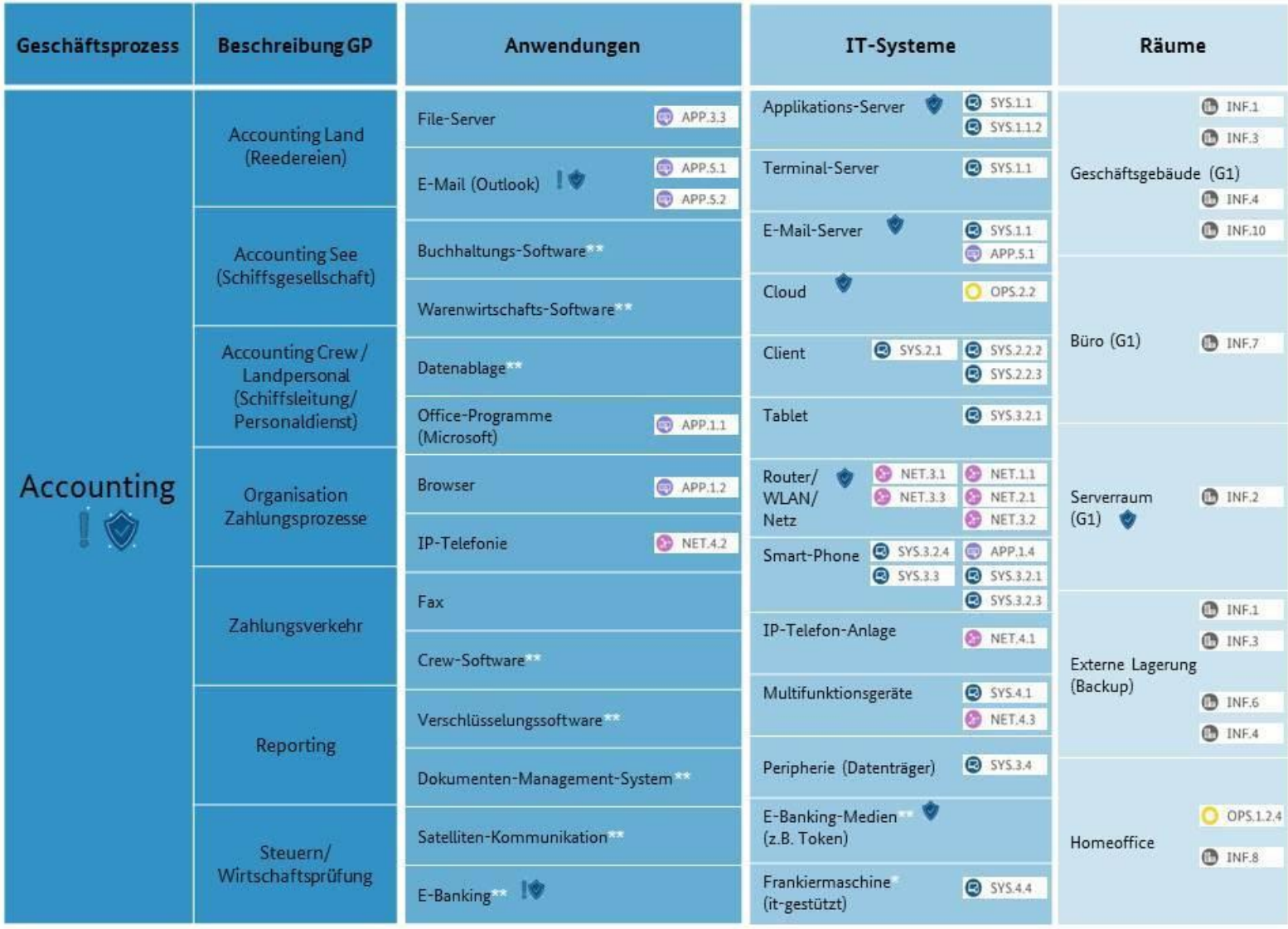
- **Address the risks**
  Generally, your risk assessment will show that your existing security does not adequately cover all threats. In this case, you need to consider how to adequately address the remaining threats and make a reasoned decision to follow up on this.
- **Consolidate the security concept**
  As a conclusion to the risk analysis, the additional measures you have decided to implement need to be integrated into the existing security concept (= consolidation of the security concept) and the security process continued on the basis of this.

14 Annex

The maps of the two business processes discussed here:

- Business Process: 'Accounting' (14.1)
- Business process: 'Technical Management' (14.2)

14.1 Annex 1: Business process map – ‘Accounting’



14.2 Annex 2: Business process map – 'Technical Management'