Information Security Officer: Job profile, necessary qualifications, and awareness raising explained in a practical way

Basis: ISO/IEC 2700x, BSI Standards 200-x, and IT-Grundschutz Compendium

Gefördert von
HGS Horst Görtz Stiftung

Technische Hochschule Wildau
Technical University of Applied Sciences
WILDAU

Margit Scholl (ed.)

Information Security Officer:
Job profile, necessary qualifications, and awareness raising explained in a practical way

Information Security Officer:
Job profile, necessary qualifications, and awareness raising explained in a practical way

Basis:

ISO/IEC 2700x, BSI Standards 200-x, and IT-Grundschutz Compendium

Prof. Margit Christa Scholl, PhD

Business computing and administrative informatics
Faculty of Business, Computing, and Law
Technical University of Applied Sciences Wildau (TH Wildau)

Ernst-Peter Ehrlich

Laboratory engineer
Faculty of Business, Computing, and Law
Technical University of Applied Sciences Wildau (TH Wildau)

Buchwelten Verlag
FRANKFURT AM MAIN

Bibliographic information from the German National Library

The German National Library lists this publication in the Deutsche
National bibliography; detailed bibliographical data is available on the Internet
http://dnb.d-nb.de available.

The printing of this book was funded by the Horst Görtz Foundation (HGS) as part of the project “Information Security Awareness for Everyday School Life (SecAware4school).”

Imprint
Information Security Officer:
Job profile, necessary qualifications, and
awareness raising explained in a practical way

© Published by
Bubans Buchwelten Verlag
60437 Frankfurt am Main
https://www.buchwelten-verlag.de

Copyediting: Simon Cowper

Download additional image files, posters, and graphics at
https://www.buchwelten-verlag.de/dl/29105/content/iso2020.zip

ISBN: 978-3-945740-12-5

The Authors

Prof. Margit Christa Scholl, PhD

Actively engaged in research since 1981; professor since 1994, at TH Wildau since 1997

Professor for business computing and administrative informatics and head of the laboratory for administrative informatics at TH Wildau since 2001

Founder (2010) and director of the Wildau Institute for Innovative Teaching, Lifelong Learning, and Creative Evaluation (WILLE) in the Technology Transfer and Continuing Education Center (TWZ e.V.) at TH Wildau

Qualification partner of the Federal Academy of Public Administration (BAköV) at TH Wildau:

- Since 2010, advanced training course with certification exam “IT Security Officer I”
- Since 2017, advanced training course with certification exam “Data Protection Officer in Compliance with the EU GDPR”

Since 2018, advanced training course with certification exam as “Security Awareness Officer” based on research findings from her research team and project partners

Since 2019, basic training “IT-Grundschutz Practicioner” in line with the requirements of the Federal Office for Information Security (BSI)

Since 2019, advanced training "IT-Grundschutz Consultant" in line with the requirements of the Federal Office for Information Security (BSI)

Since 2016, DLGI test center for the International/European computer driving license (ICDL/ECDL) and the data protection driving license

Ernst-Peter Ehrlich

Laboratory engineer in the Faculty of Business, Computing, and Law, active in Prof. Scholl’s laboratory for administrative informatics at TH Wildau since 2015

IT security officer certified in line with BAköV/BSI since 2014

- Implementation of technical training/exercises in the field of data protection, and
- IT security and DLGI tests for the ICDL/ECDL and the data protection driving license

Training courses and awareness-raising events can be booked through the Technology Transfer and Continuing Education Center at TH Wildau (TWZ e.V.), at the Wildau Institute for Innovative Teaching, Lifelong Learning and Design Evaluation (WILLE):

https://twz-ev.org/institute/wildau-institut-fuer-innovative-lehre-lebenslanges-machen-und-gestaltende-evaluation/#tab-id-1

The following symbols are used in the book to denote specific passages of text:

Organization		**Training information** Here we refer to factors that should be kept in mind when the training is being organized and suggest particular aspects that require focus during planning.
Theory		**Notes on theory and literature** The literature we use in the book is shown in full at the end in a reference list. This symbol is used to draw attention to works that, in our opinion, provide particularly good theoretical explanations.
Exercises		**Recommended exercises** We use this symbol to denote descriptions of our training exercises. This can relate to individual project work or interpersonal exchanges and may include experience-oriented learning scenarios or technical instructions for software.
Definitions		**Can you explain? (Check yourself)** Terms or situations that readers should be familiar with after study and practice are summarized under this symbol as a tool for self-testing.
Practical examples		**Practical examples for administrations, companies, and institutions** Here we list practical suggestions and examples accompanied by specific instructions wherever possible.
Note		**(Personal) watch list** We use this symbol to draw attention to important things. In addition, each chapter ends with space for your own list.
Idea		**(Personal) ideas** We use this symbol to draw attention to a good idea. In addition, each chapter ends with space for your own ideas.
Summary		**(Personal) summary** We use this symbol for our short summary. Each chapter also ends with a space for a personal summary.
Advantages/ disadvantages		**What are the advantages/disadvantages in terms of content?** After reading each chapter, you may notice certain advantages and disadvantages in how things are organized in your institution. There is room for you to make a note of this!

Acknowledgements

At this point, we would like to thank all of you who supported and motivated us during the production of this book. Understanding the importance of information security and raising the level of awareness (information security awareness) for every individual can only succeed if there is an exchange with helpful suggestions and constructive criticism. We thank SerNet GmbH, Berlin, for their feedback on our tutorial covering the software-based development of a security concept using the *verinice* tool. We would like to thank Dietmar Pokoyski (known_sense) for his imaginative support as a contractor in our projects.

We are very grateful for input from the "Research Group Scholl" at TH Wildau in its 2019/2020 incarnation and would like to recognize the following individuals for their steadfast commitment: Denis Edich, Josephine Gerlach, Stefanie Gube, Peter Koppatz, Frauke Prott, and Regina Schuktomow. We are also grateful to the staff of the research group for their input over the past years.

Special thanks go to Stefan Borchert, who, as engineer for Prof. Scholl's laboratory for administrative informatics at TH Wildau, provided creative support in the development of the BAköV/BSI qualification course from 2010 to 2014.

We would like to thank the Horst Görtz Foundation (HGS), and especially Dr. Görtz, for providing external funding for our research and the printing of this book.

Margit Christa Scholl and Ernst-Peter Ehrlich

Wildau, July 2020

Content

Foreword

The Federal Academy of Public Administration within the Federal Ministry of the Interior, Building, and Community (BAköV) has been working with the Federal Office for Information Security (BSI) since 2007 to train and certify IT security officers (IT-SO) for public administration. This successful concept has so far been adopted by only a few universities as part of their training and further education program. This is probably because the concept and certification relate to public administration, and to federal administration in particular. Under my leadership, the Technical University of Applied Sciences Wildau (TH Wildau), where administrative courses have been an established part of the curriculum since 1997, adopted this certification concept in 2010 and focused on its successful implementation in an appropriate form. From the start, the aim was to make a significant contribution to the quality of information security in the Brandenburg region and beyond. After attaining recognition as a BAköV qualification body, I have since expanded this training for students from a wide variety of courses and for external employees. The course's content and methodology have been continuously updated. Having integrated information security in the different courses, especially in non-technical contexts, TH Wildau is undoubtedly a pioneer in the field. The certification of students at TH Wildau was funded by the Horst Görtz Foundation (HGS) in the period 2018 to 2020.

With almost 3,700 students, TH Wildau is the largest (technical) University of Applied Sciences in the state of Brandenburg. Its attractive range of courses currently comprises forty-one bachelor's and master's courses in science and engineering as well as in economic, administrative, and legal disciplines. Another special feature of the university is its internationality. Some 25 percent of the students come from more than sixty countries. Partnership agreements and student and lecturer exchanges connect TH Wildau with over 140 academic educational institutions worldwide. The university has had a top position in applied research nationwide for years and has a recognized reputation as a center of excellence for important scientific disciplines. We are pleased to have a productive ongoing cooperation with the BAköV and the BSI that provides education and training in information security and helps raise awareness of the topic.

Our range of further training courses and the final certification are based on a manual that was created by the BAköV and the BSI in cooperation with the Fraunhofer Institute for Secure Information Technology (SIT) and is currently available in a revised version 6.2 [1]. This manual is not public and can only be obtained as part of the BAköV/BSI training. The contents of the manual may only be used in consultation with the BAköV. In devising this book, we have no intention of reduplicating this manual. Rather, we want to acquaint our readers with our diversity of experience in the *implementation* of further education in information security, with the aim of integrating theory and practice. This ranges from the individuals responsible for and involved in security management to the designated information security officers, who are also required to initiate qualification measures themselves as part of their function. We essentially refer to publicly available sources, in particular the international family of standards for information security ISO/IEC 2700x, the national BSI Standards 200-x, and the IT baseline protection (*IT-Grundschutz Compendium*). To ensure a consistent level of security, it is increasingly important that information security officers (ISO) are properly qualified. It is therefore necessary that this group of people has a defined and solid body of specialist knowledge, a sound training, and the option of obtaining the relevant certification.

This includes consideration of how an abstract, theoretical understanding of security information can be conveyed to participants in an advanced training course in a clear and understandable way. The quality of our advanced training with certification is ensured by current, practice-oriented knowledge transfer with interactive and participative teaching/learning methods.

This is supported by the size of the classes, which are limited to a maximum of eight participants. Here, there is also the possibility of individual design, depending on the specific needs of the participants. This makes the design of the training flexible and takes into account the previous knowledge, professional experience, and areas of responsibility of the target group. Participants also have the opportunity to exchange ideas grounded in their previous experience as a means to solve challenges. Psychologically based research results in the fledgling discipline of corporate information security suggest this is a crucial element in raising awareness in learners with long-lasting effect [2].

In this respect, all the activities undertaken by my research group "Information Security Awareness" in developing and applying methods and tools for raising awareness and training in information security are important for this book—these have been incorporated into teaching and training for years. At the meeting of the BAköV's and BSI's partners at TH Wildau in 2017, for example, the participants were impressed by the extensive results of my research group—especially by the way experience-oriented analog and digital learning scenarios on current risk situations such as phishing, password hacking, and social engineering can be integrated into teaching and further training. Such examples from our research projects with different target groups as well as ideas from student projects should also be outlined here as a suggestion for ISOs to raise the awareness of colleagues. In advanced training courses, such experience-based and game-based learning scenarios can be used as an effective warm-up tool with a serious background, while at the same time serving to consolidate knowledge.

To ensure a high level of security in all institutions, whether public or private, the ISOs and everyone responsible for information security must be properly qualified. Ernst-Peter Ehrlich has supported me as a lab engineer in my laboratory for media-integrated administrative informatics at TH Wildau since 2015 and actively contributed to the implementation of the advanced training courses with certification. He is specialized in technical training exercises and also provides valuable input for all readers in this book, especially if they want to or need to work actively as ISOs.

It is hoped that this book will enrich the methodology of further training in information security: our experience-oriented scenarios and the teaching we offer in discursive didactics aim to engage participants in communication and discussion as a basis for action.

Prof. Margit Scholl, PhD

Wildau, July 2020

1. A roadmap and the BSI “IT-Grundschutz” brought up to date

1.1 Introduction

There are a wide range of questions to be considered with regard to information security (IS). Not only do technical and organizational problems need to be clarified but legal, economic, and social answers must also be found. The growth in IS is an increasingly important factor in all institutions as digitization becomes increasingly prevalent. Security is crucial to any organization, as is the competence of those responsible for it—*IT security officers* (ITSOs) or *information security officers* (ISOs)—as well as all the tasks that fall within the remit of information security management (ISM).

Norms and standards define the establishment, development, and maintenance of an institution’s information security management system (ISMS) as well as its certification processes. Beyond delineating the importance and purpose of IS, they also specify the roles that should be filled in an institution if an ISMS is to be successful. This extends to the appointment of relevant staff. However, the people concerned are often not aware of the tasks involved and their specific functions, while the procedures themselves may also be unclear. This book attempts to shed light on this.

At the meeting of the BAköV qualification partners with the BSI in 2011, a roadmap was discussed to facilitate the creation of an implementation plan catering to the minimum IS requirements for the federal administration (in German: *UP Bund*). On the basis of this roadmap and the updated basic protection program, we have developed a new overview (see fig. 1 and table 1) which, to the best of our knowledge, can be used as a “common guideline” for all institutions. In the following chapters, we will refer to this figure and table again with regard to the specific topics under consideration in order to provide readers with a practical way of building a security concept and culture in an institution.

In the upper part of fig. 1, the project management milestones are shown for the creation of an ISMS. Table 1 (continued in part 3) shows that an institution’s Business Continuity Management (BCM) can be established in parallel from the start. The areas of responsibility for the key staff are also listed in table 1. Such a complex project is usually made public with a kick-off meeting, in order to make everyone involved aware of the vision, goals, and scope of the project (see fig. 1 and table 1). A project usually ends when the results are put into operation: thereafter, the concepts and processes in the institution should be continuously improved while an ISMS and a BCM are being set up in accordance with the relevant standards and norms (see chapter 2).

Before the actual ISMS and BCM projects begin, the business processes must be identified, analyzed, and modeled, because they form the starting point for both the security and the emergency concept.

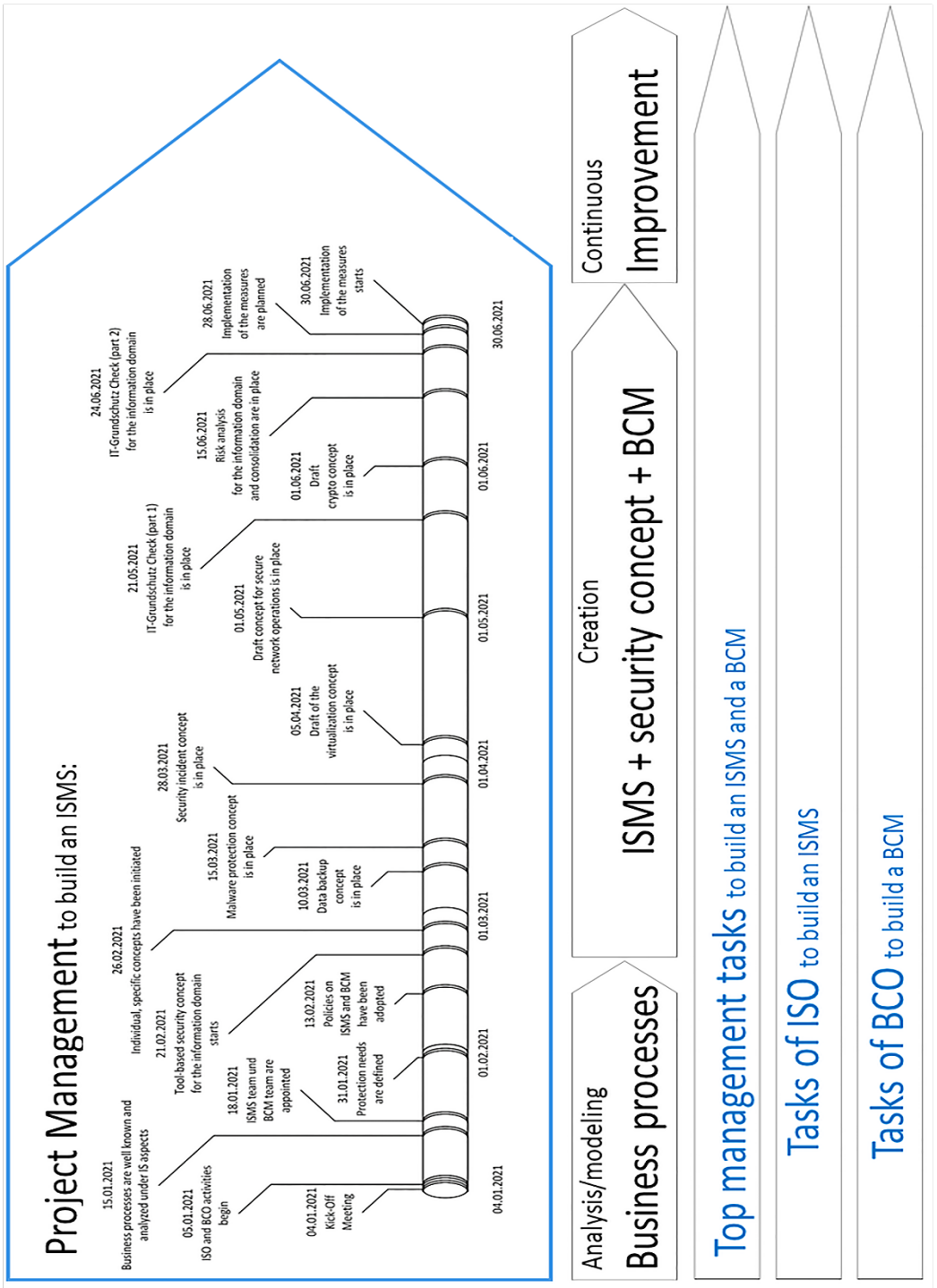


Fig. 1 Graphic roadmap for setting up an "Information Security Management System (ISMS)" and "Business Continuity Management (BCM)" framework in an institution (see table 1).

An idealized project schedule for a small institution with manageable business processes and a limited information network as well as comprehensive availability for all actors. The BCM can also be set up in parallel to the ISMS with its security process and the development of the security concept. In both cases, the business processes must already be identified and known—this is usually the responsibility of the organization, as well as the management. With ISMS, the business processes are necessary for the definition of protection requirements specific to the organization (see chapters 2 and 3). With BCM, the business processes are important for the so-called Business Impact Analysis (BIA), which is dealt with in chapter 6. The information security officer (ISO) and business continuity officer (BCO) begin their duties after their official appointment.

The top management of an institution is responsible for the initiation of projects and the appointment of an ISO and business continuity officer (BCO) right at the start of the process. As per fig. 1 and table 1, it should be noted that the BCM can also be set up in parallel to setting up an ISMS (it does not need to wait until afterwards!). In practice, it means that the ISO takes care of the general control and coordination of the entire security process and the creation of security concepts right across the institution. At the same time, the BCO focuses on critical business processes in order to ensure continuous operation, especially of these critical functions. This also includes the development of emergency preparedness concepts and emergency plans.

Level 1	Level 2
Project Management	Kick-off meeting is held.
	ISO work is started.
	BCO work is started.
	ISMS team is appointed.
	BCM team is appointed.
	IS policy is published.
	IS protection needs are defined.
	Individual, specific IS concepts are created.
	Security guidelines are created.
	An entire security concept is created for the information network.
	Measures are implemented to establish IS.
	IS is revised to ensure basic security.
	Emergency management is put in place.
Top Management	Management has a knowledge of the core business processes, which are identified and analyzed from an IS perspective. Project is initiated and expounded so it can serve as a model.
	IS goals and strategy are developed.
	The entire IS strategy is aligned with the business processes.
	ISO is appointed.
	BCO is appointed.
	Management assumes overall responsibility for IS.
	Resources are made available.
	IS policy is initiated.
	IS policy is checked and signed off on.
	Monitoring of the overall IS process is initiated.
	Ongoing responsibility is assumed when reviewing IS reports.
	Management support is ascertained for the security process.

Tab. 1 Part 1: Important milestones of a roadmap for setting up an "Information Security Management System (ISMS)" and a "Business Continuity Management (BCM)" framework in an institution, presented from the point of view of the general project management and showing the tasks of top management. Level 1 indicates the particular role, while level 2 lists the associated milestones.

Level 1	Level 2	Level 3	Level 4
ISO Coordination	Further education and training ISMS	Carry out personal ISO training.	
		Develop IS training concept for the institution.	
		Initiate IS awareness and training measures, possibly after tendering; carry out in-house as necessary.	
	Framework ISMS	Design the IS policy.	
		Participate in the ISMS organization.	
		Plan ISMS resources.	
	ISMS reporting to the top management	Plan reporting for IS.	
		Plan information reports for employees.	
		Schedule reports for technical personnel.	
	ISMS protection level	Clarify basic, core, or standard protection approach.	
		Clarify information domain.	
	ISMS security concept	Implement specific concepts.	Data backup concept is in place.
			Malware protection concept is in place.
			Security incident handling is in place.
			Concept for virtualization is in place.
			Concept for secure network operation is in place.
			Encryption concept is in place.
		Create security guidelines for the individual, specific concepts.	
			Security guidelines are in place.
	Create security concept	Choose a support tool.	Support tool is selected.
		Set up information domain.	Information domain is in place.
		Analyze structure of the information domain.	
		Determine protection requirements for the information domain.	
		Model the information domain.	
		Perform IT-Grundschutz check (part 1) of the information domain.	
		Carry out implementation planning (part 1).	
		Generate reports.	
		Perform risk analysis of the information network and consolidate.	
		Perform IT-Grundschutz check (part 2) of the information domain.	
		Plan implementation of measures for the information domain.	
	Plan and review continuous improvement of ISMS	Map out documentation.	Documentation is coordinated.
		Initiate quick checks.	Quick checks are in place.
		Initiate IT revision.	IT revision is integrated into everyday routines.
		Initiate penetration tests.	Penetration tests are carried out.
		Schedule continuous repetition.	Continuous review is established.
		ISMS is routine.	Full report is created.

Tab. 1 (cont.) Part 2: Important areas of responsibility for ISO as a roadmap for coordinating the establishment of an "Information Security Management System (ISMS)" in an institution. Level 1 indicates the role, while level 2 lists the main functional aspects and levels 3 and 4 specify the milestones.

Level 1	Level 2	Level 3	Level 4
BCO Coordination	Further BCM education and training	Implement in-house BCO training.	
		Develop a training concept for emergency preparedness.	
		Initiate training measures.	
BCM framework		Design BCM policy.	BCM policy is in place.
		Design structure of the BCM organization.	Structure of the BCM organization is in place.
		Plan BCM resources.	BCM resources are approved.
		Write BCM reports for top management.	Plan and complete management reports.
		Reporting is in place targeted to specific groups.	Staff have access to continuous information.
			Ongoing technical staff reports are generated.
Development of the emergency preparedness for the institution Coordinated creation of the emergency concept		Create concept in collaboration.	Set up coordination with all actors in the institution. Set up participation in the emergency organization.
		Plan implementation.	Schedule is in place.
		Plan emergency response.	Practice exercises are carried out.
		Plan evaluation.	Practice exercises are evaluated.
		Emergency concept is in place.	Report is created.
Plan and review continuous improvement of BCM		Schedule continuous repetition.	Continuous review process is established.
		Plan revision.	Revision is integrated into everyday routines.
		Overall concept is in place.	Full report is created.

Tab. 1 (cont.) Part 3: Important areas of responsibility for business continuity officers (BCO) as a roadmap for coordinating the establishment of a "Business Continuity Management (BCM)" in an institution. Level 1 indicates the role, while level 2 lists the main functional aspects and levels 3 and 4 specify the milestones.

When the ISO and BCO are *appointed* by the top management, their qualifications and basic training must be verified. In practice, resources such as time and money are necessary and must be provided by the institution. The management of the institution bears the overall responsibility for the business processes, the ISM, and the BCM. In addition, the executives of an institution need to act as role models from a security point of view—in practice, this is not obvious to all executives. An institution's security regulations apply to everyone and must be made clear to everyone, which is why the awareness-raising and training measures are extremely important. These should not be underestimated (see chapter 4).

Top management, executives, and ultimately all employees must be continuously informed about the specific security situation in their institution and for the specific context in which they work. In agreement with the management, ISO and BCO therefore have to set up a meaningful reporting system targeted to specific groups (see fig. 1 and table 1, parts 2 and 3). In addition, it should be made clear that ISM and BCM involve a continuous improvement process that in practice is known in all areas of management as a Plan-Do-Check-Act (PDCA) cycle or Deming model [3] [4].

Continuous improvement is necessary because the work of institutions and their employees is fluid, estimated risks may change, and concepts need to be re-evaluated accordingly. According to Arne Schönbohm (2016), president of the BSI, the "IT-Grundschutz of the BSI is the proven method for establishing a solid management system for information security in companies and administration. The dynamic area of information security, a new political framework, such as the IT security law, and the needs of users were the deciding factors in necessitating a fundamental revision of the IT-Grundschutz" [5]. This fundamental revision is referred to as modernization. The first edition of the updated ("modernized") IT-Grundschutz was presented by the BSI in October 2017 after an intensive development process in which users, IT and information security officers, and auditors and tool manufacturers were involved.

The modernization of the IT-Grundschutz affected

- the BSI *Standards for the ISM*, which in addition to changes in content also received the new numbering 200-1, 200-2, and 200-3, and
- the IT-Grundschutz catalogs, which contained the individual IT-Grundschutz modules and have now been replaced by the *IT-Grundschutz Compendium*, which contains the updated modules in a new grouping and leaner text form.

The BSI standards, which are also based on the international ISM standards (ISO/IEC 2700x), and the *IT-Grundschutz Compendium* are supplemented by the

- implementation instructions for the individual IT-Grundschutz modules, in which the options for fulfilling the requirements of a module are described based on recognized best practices, and
- the IT-Grundschutz profiles, in which model solutions for the application of IT-Grundschutz are shown for selected application scenarios.

Overall, the modernization of IT-Grundschutz should make its methodology and recommended measures more flexible and efficient, so that they can be used in different institutional sizes and application scenarios and more easily adapted to changing technical conditions.

"The goal of modernization [of the BSI IT-Grundschutz] is to enable small and medium-sized companies [SMEs] in particular to easily get started with their own security management." The German IT-Grundschutz is too complex, which is why new forms of entry have been defined (see fig. 2): there is now a basic entry and a core entry, in addition to the familiar standard entry.

The first step in security management is *basic* security, which, however, is not sufficient for the certification of an institution—see fig. 2 and table 1 (cont.), part 2. With *core* protection, the focus is on key selected areas—i.e., particularly sensitive business processes—whose protection requirements are high to very high.

Classic *standard* protection addresses a normal need for protection and corresponds to the previous procedure for IT-Grundschutz. It also enables the certification of an institution according to the international standard ISO/IEC 27001. Norms and standards for IS should be familiar to the ISO (chapter 2). We examine the standard protection in this book because this is the only means to actually protect an institution with a normal level of protection requirements, and, moreover, this level guarantees certification according to ISO/IEC 27001. On the other hand, we see that starting with basic protection is more straightforward, even if the effort involved should not, in the end, be underestimated. Even more noteworthy is the input required for core protection, which will only relate to a limited area of the institution and can also be certified separately. We cover the tool-based development of a security concept in terms of standard protection in chapter 3, where it is looked at step by step.

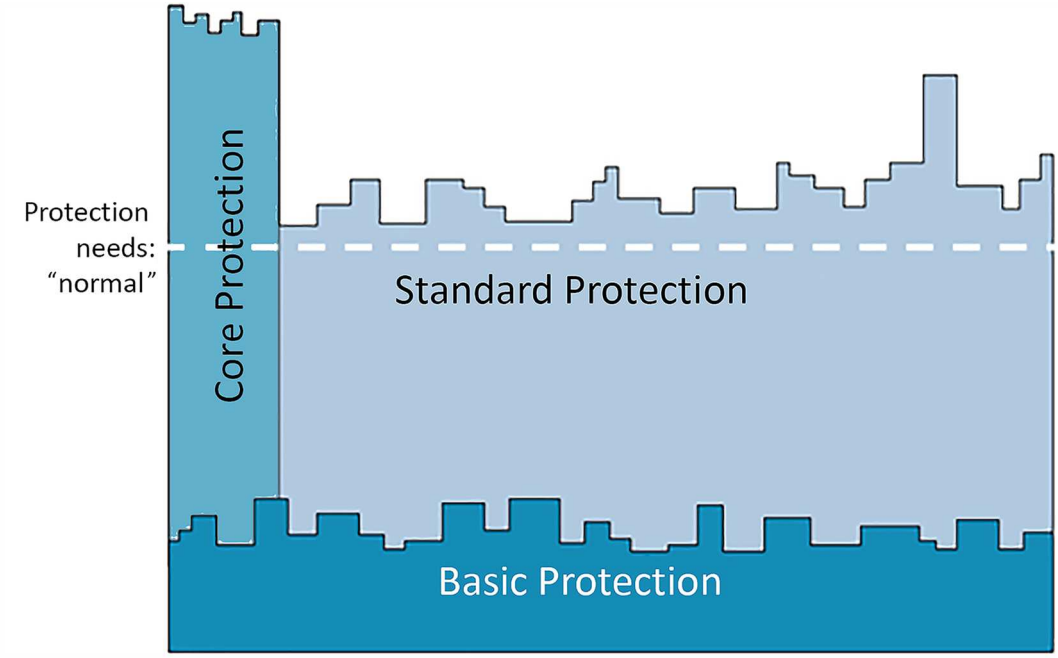


Fig. 2 *The new procedures of the BSI's updated ("modernized") IT-Grundschutz. They comprise three different types of protection and are intended to facilitate entry into IT-Grundschutz (original image source: BSI [5]).*

Guaranteeing *normal protection* is achieved in IT-Grundschutz by attending to the three basic values of IS—confidentiality, integrity, and availability. We illustrate this in the tool-based development of the security concept for standard protection in chapter 3. *Confidentiality* requires protection against the unauthorized disclosure or perusal of information. *Integrity* means ensuring the correctness of information and the correct functioning of systems. *Availability* relates to the use of services, information, IT systems, applications, and networks by the user at the scheduled or (contractually) agreed times.

Since the term *information security* is more comprehensive than the term *IT security* and focuses on the protection of information of all types and origins [1], we use the term ISO and not IT-SO in this book, as per the updated BSI standards.

However, personal BAköV/BSI-based certification remains unaffected as long as the BAköV adheres to the term IT-SO with a certificate in its advanced training course “IT security officers in public administration.”

What importance do ISOs have in an institution and what tasks do they perform? To answer this question, we refer to fig. 1, where it explicitly states that they, along with the top management of an institution, are responsible not only for the IS or ISM but also for determining the remit of the ISMS. This includes the appointment of an ISO, depending on the size of the institution, even if it is not currently required by law in all institutions. The BSI and the BAköV recommend the organizational integration of the top management as a staff unit [1] with responsibility for all questions and activities of the institution related to IS. This includes coordinating participation in the development of concepts and guidelines as well as the orchestrated selection of specific security measures.

ISOs should base their work on recognized international norms and national standards for IS. According to the BSI, this ensures that nothing important is overlooked and facilitates coordination between those responsible for the necessary security measures. Meanwhile, the compilation of “Best Practices” provides a great deal of information on how to ensure that the work required to implement IS within the institution remains within the bounds of what is reasonable. This is looked at in theoretical terms in chapter 2 and run as an explicit practical task in chapter 3 using the tool-based structure of a security concept for a defined information network.

ISOs should also be able to assess possible threats and their relevance for their own institution using risk management. Chapters 2 and 3 provide information on this. Checking the effectiveness and appropriateness of the concepts, guidelines, and measures is also part of the ISO remit. The so-called IS revision is an important tool, for example, for advancing the security process and supporting the ISM and ISO in their work. In addition, IS revision is a procedure for quickly assessing the IS status and associated processes in an institution. This gives ISOs an overview and information on the targeted use of the available resources [1].

In order to successfully fulfill their function, ISOs thus need solid specialist knowledge that can be acquired through appropriate in-house training (see table 1), and this should be planned as part of making the appointment. Chapters 2 and 3 therefore contain questions and ideas under the heading Implementation Aspects and Exercises both for training ISOs and for raising awareness among employees and managers. In addition, ISOs need detailed knowledge of the structures and processes of the institution because they should be able to analyze and formulate IS requirements in the context of business process requirements (see fig. 1 and table 1).

Because of the need to coordinate a variety of processes with different actors, ISOs need strong communication skills.

In addition, the ISO is tasked with developing a training concept for specific groups right across the institution and initiating, commissioning, or personally carrying out appropriate awareness-raising and training measures and reviewing their success. Awareness-raising measures are intended to holistically attune management and all employees to the issues involved: these measures are explained in more detail in chapter 4.

In-depth training measures are intended to promote the necessary fields of competence in the institution, which are necessary for the efficient use of the potentials of IT and include the establishment of comprehensive information security competence. The ISO also needs extensive knowledge of the various aspects of IS. You should know which technical and organizational measures (TOM) can be used to adequately counteract the dangers and therefore require a basic understanding of the functioning of information technology systems.

In chapter 4, therefore, we have summarized important findings for the awareness-raising and training concepts in institutions, while in chapter 5 we take as examples key areas that the ISO should be familiar with. ISOs can obtain a variety of information, suggestions, and downloads for their work via the BSI website.

In chapter 6, we present important aspects of emergency management in line with BSI Standard 100-4 and refer to its modernization, which is still ongoing. Overall, business continuity officers (BCOs), information security officers (ISOs), and data protection officers (DPOs) should work hand in hand when setting up an institution's security system while at the same time addressing different security angles.

In this book, we use certain symbols, which were explained at the beginning, to enable a quick overview and clarify our discursive didactics. The symbols are intended to give readers ideas for communicative participation and lead to a certain amount of argument-based activity as they read. We use them not only to point out important or interesting things but also to inspire readers to actively work with the book and to take notes. At the end of the following chapters, we ask ISOs questions that readers should be able to answer.

We are open to improvements and additions to this book and look forward to your submissions/comments.

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

1.2 Summary of the ISO's range of tasks

The business processes of an institution nowadays are almost completely dependent on the secure and flawless operation of IT. The activities and skills of the ISO and the entire ISMS team are of key importance for an institution. In order to be able to perform their tasks appropriately, ISOs need extensive knowledge of the various IS aspects. Therefore, they also require well-grounded, ongoing advanced training. For example, you should be able to assess possible threats and their relevance for your own institution. They should also know what technical and organizational measures (TOM) can be used to counter the threats appropriately and effectively. They also have to have very good communication skills because in IS terms they represent the link between very different roles in the institution. They thus need to be able to communicate very well with the management, the managers, the employees in general, and the administrators in particular if an effective ISMS is to be set up in the institution. The typical tasks of an ISMS, such as the creation of the policy and additional guidelines, the development of an appropriate organizational structure for IS, the risks associated with performing specialist tasks, and the topic of security revision often need to be made clear to the management first.

The goals, business processes, and areas of responsibility of an institution are also subject to change, as are the available resources, organizational structures, and external conditions. The precautions required to ensure IS must thus be continuously adapted to changing conditions. Once a security level has been reached, it should be maintained and enhanced rather than being allowed to deteriorate. Therefore, new security measures must be implemented and those that have been implemented must be checked regularly by the ISO for their effectiveness and appropriateness. Their applicability and actual usage must be verified. After changes have been made, and in light of security incidents, identified weaknesses, and gaps, the measures must also be adjusted and improved. The adjustments must once again be planned, implemented, and checked. It is important to obtain broad acceptance for the measures at management level and among employees.

The primary job of the ISO is to control and coordinate tasks to create a security concept with associated sub-concepts, guidelines, and regulations. They play a supporting role vis-à-vis the management of an institution and must initiate and review tasks for the implementation of the security measures. They should help shape an effective security process and practice efficient reporting. In addition, security-relevant IT failures, malfunctions, and effects must be investigated and awareness-raising and training measures for IS should be initiated, planned, and coordinated.

Fig. 3 *Poster made by the Research Group Scholl (FS) showing lists of tasks based on the BSI standards [12], IT-Grundschutz [5], and the BAköV manual [1]. Important areas of ISO responsibility and the basic values of information security and other protection goals are mentioned. The summary covers the areas of malware and common forms of attack, threats to stored data, data backup requirements, active and passive components of network technology, protective measures—both in general and specifically for mobile devices—mail client security and encryption methods, legal violations (StGB offenses), BSI tasks, BSI standards, and IT-Grundschutz modules and procedures.*

The poster can be downloaded as a PDF from the book's download area (Password: iso2020).

2. Standards and norms for information security: Basis of an institution's security concept

2.1 The international series of standards ISO/IEC 2700x for IS

As the word *series* suggests, ISO/IEC 2700x is a combination of various standards focused on the management of information security. As they are norms, these documents have undergone a standardization process and are also published in some cases as German DIN standards. In this context, the abbreviation ISO stands for *International Organization for Standardization* and IEC for *International Electrotechnical Commission*. This "ISMS family of standards" [6] deals with basic requirements and measures for setting up, operating, and developing an information security management system (ISMS). An overview of the current standards can be found in fig. 4.

The ISO/IEC 27000 standard was first published in 2009 and updated in 2012, 2014, 2016, and 2018. It contains an overview of the principles, concepts, and terms relating to ISMS, and introduces the family of standards containing the current norms. The fifth edition from 2018 is available from ITTF as a free download (PDF for individual users) in English and French [6].

The ISO/IEC 27001 standard generally describes the requirements for the procedure for introducing and maintaining an ISMS in the context of an institution (see [8], for example). What is special about this standard is that it makes an institutional *certification* possible. If an institution claims conformity with the ISO/IEC 27001 standard, it must be compliant with all of the requirements described in it. The requirements relate to the organization, management, planning, support, operation, evaluation, and continuous improvement of the ISMS. In Annex A of the standard, reference measures and the objectives associated with them are identified in fourteen sections, which must be applied accordingly by an institution in the context of information security risk treatment. Information security officers (ISOs) should be aware of the IS norms as a basis of their work and as a support in arguing for it. For example, the description of an ISMS according to ISO/IEC 27001 pursues a *holistic* view of the risks associated with an institution's IS and can be used to illustrate the range of a security team's work. The standard also describes the *coordinated* introduction of measures to increase IS for the business processes of the institution and can be used by ISOs to clarify their role as coordinators.

The ISO/IEC 27002 standard's title is *Code of practice for information security controls* and specifies these security measures as a compilation of best practices, which in version 2017-06 [8] are divided into the fourteen sections (or *security control clauses*) mentioned in the appendix to ISO/IEC 27001, with thirty-five *main security categories* and a total of 114 *security controls*—i.e., individual measures. The connections to these standards are set out as examples in the following chapters.

We also consider the ISO/IEC 27004 standard to be important for ISOs. It deals with monitoring, measurement, analysis, and evaluation. This standard describes in general, how the institution can check the actual success of an ISMS on the basis of key figures and their measurement. This is of particular importance since our own research indicated significant shortcomings in this area [9]. Guidelines for IS risk management are summarized in the ISO/IEC 27005 standard. This standard is of particular importance for managers and employees dealing with risk management within institutions and for external service providers who support such activities.

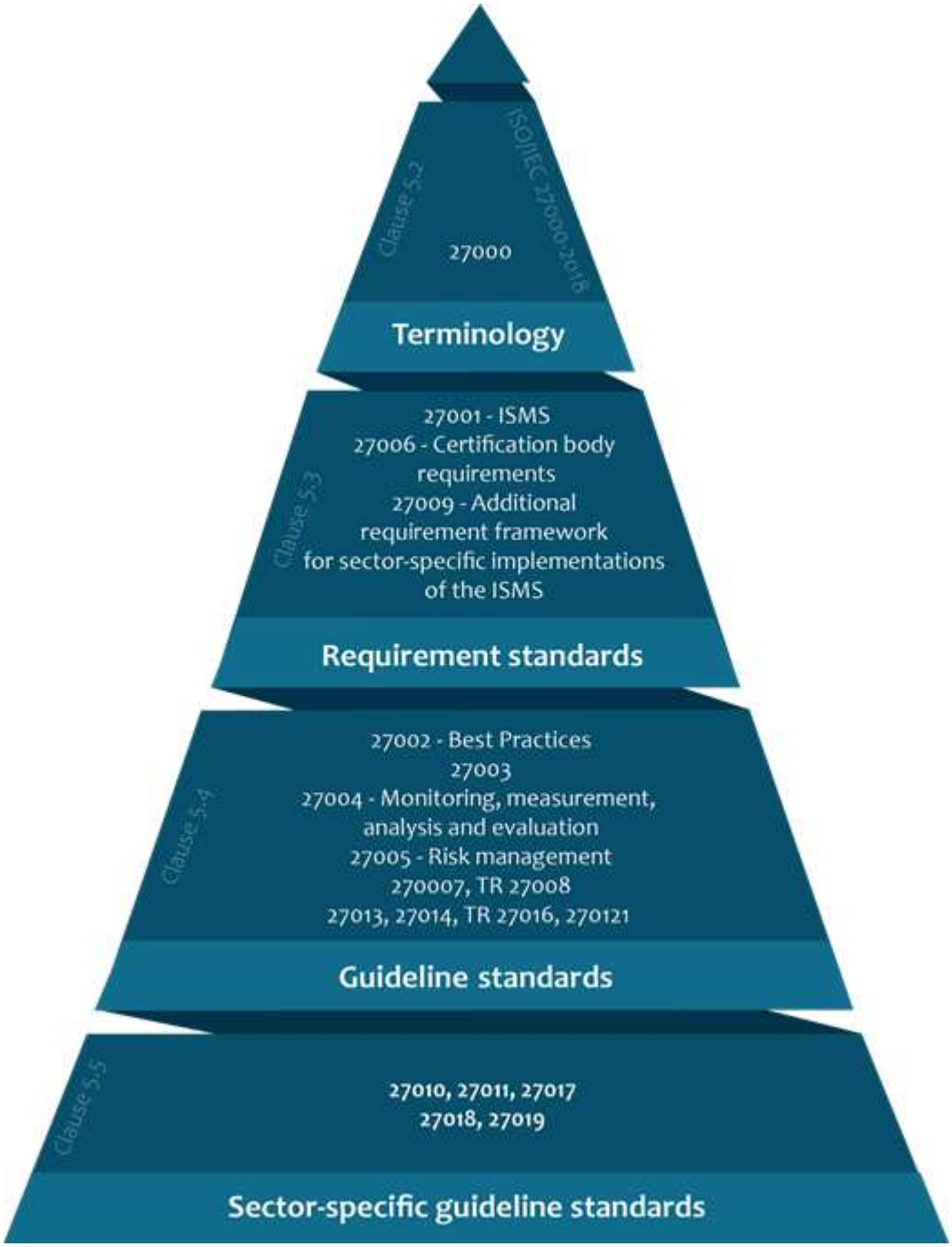


Fig. 4 ISMS family of standards for establishing an information security management system (ISMS) based on ISO/IEC 27000. Author's illustration in line with [6] and [7].

Detailed knowledge of the other standards of the ISMS family ISO/IEC 2700x is useful, or indeed necessary, for specific situations or for specific institutions—for example, for the ISMS certification processes or for the accreditation of certification bodies for ISMS or for cloud standards. However, such standards are not the subject of this book.

Implementation and training exercises

The international ISMS family of standards ISO/IEC 2700x is also important as a basis for the German BSI standards and all the tasks ISOs have to deal with. However, conveying the content of these standards with a wealth of terms, definitions, and requirements is a rather "dry" affair. This kind of approach in frontal teaching methods does not necessarily give learners the ability to put the content into practice.

It is therefore better to have the participants be active themselves. If possible, they should be given the opportunity to "browse" the standards themselves. Moreover, they should be able to exchange ideas based on a range of different questions. For example, the question "What are the essential elements involved in building the ISMS of an institution in line with ISO/IEC 27001?" can be answered just by using the table of contents of this standard.

Below are some further examples of questions for exercises based on the ISMS family of standards ISO/IEC 2700x are:

- Can you, as an ISO, **request** a further training from management according to ISO/IEC 27001?
- **How** could you, as an ISO, carry out your job of checking whether employees have sufficient competence for the specific activities related to the ISMS?
- **What IS-related responsibilities** and authorizations must the top management of an institution give their backing to?
- **What impact** does chapter 4.2 of the ISO/IEC 27001 standard, which deals with the perception of the needs and expectations of interested parties, have on the work of ISOs?
- **What measures** does ISO/IEC 27002 propose to ensure that employees and contractors understand their responsibilities and are suitable for the intended roles?
- **What measures** does ISO/IEC 27002 set out for management and for employees (possibly including contractors) to ensure that that they are aware of and comply with their IS-related responsibilities?
- **What measures** are specified by ISO/IEC 27002 to ensure information security when mobile devices are being used?

Another way of involving participants is to exchange ideas about the sequence of steps required to set up an ISMS in the institution in line with ISO/IEC 27001. The participants can create a flowchart similar to fig. 5.

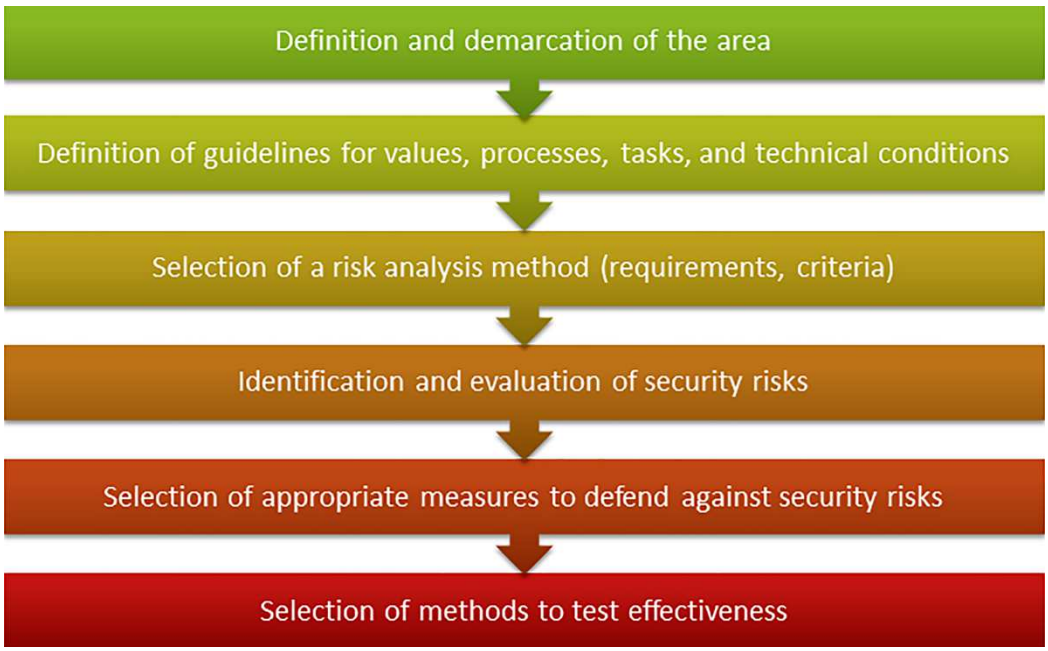


Fig. 5 Author's representation of a sequence of steps for setting up an ISMS in an institution according to ISO / IEC 27001 based on [1:86f.].

An additional exercise might involve drawing attention to the documents that are referenced. For example, the standard ISO/IEC 27001 in chapter 6.1.3, *information security risk treatment* (see [8]), provides an explanation of an important document: the statement of applicability (SoA). The SoA is an essential part of an ISMS. It should be documented with explanations setting out which security measures are put in place in the institution to address the risks that have been identified and describing the manner in which these measures are implemented. The SoA is an important part of the overall documentation of an institution's ISMS, especially for certification based on ISO/IEC 27001.

For further exercises, we can recommend the literature listed under [10] and [11], although this is only available in German. The former is an entertaining summary of an ISO's range of tasks, while the latter provides an in-depth overview of the IT security management as a whole as per the standard ISO/IEC 27001.

Space for your personal comments

Personal checklist:

2.2 The BSI standards 200-x

The international standards ISO/IEC 27001, 27002, 27004, and 27005 as well as the modernized BSI standards for IS—200-1 (ISMS), 200-2 (IT-Grundschutz methodology), and 200-3 (risk analysis based on IT-Grundschutz)—are proven tools in practice for creating a structured and efficient procedure to increase IS appropriately and to introduce, develop, and continuously improve an ISMS in an institution.

The BSI has continuously updated and expanded its standards and, over the years, has focused more on the standards of the ISMS family ISO/IEC 2700x. Since 1994, the BSI's methodology for IS has been geared to the IT-Grundschutz, which can be adapted in a modular way to different application environments [8:184]. With the current modernization of the IT-Grundschutz, *basic* and *core* protections have been added to the traditional *standard protection* (see fig. 2). These three procedures enable the institution to gradually build up an ISM. They are supplemented by the specific IT-Grundschutz modules summarized in the *IT-Grundschutz Compendium*, which are split into two groups: process-oriented and system-oriented modules (fig. 6). As fig. 6 shows, the IT-Grundschutz Compendium has a modular design and includes process and system modules for typical business processes, applications, systems, communication connections, and infrastructure, including rooms, workplaces, and cabling [13] [20]. The IT-Grundschutz addresses all the different areas that may be found in an institution.

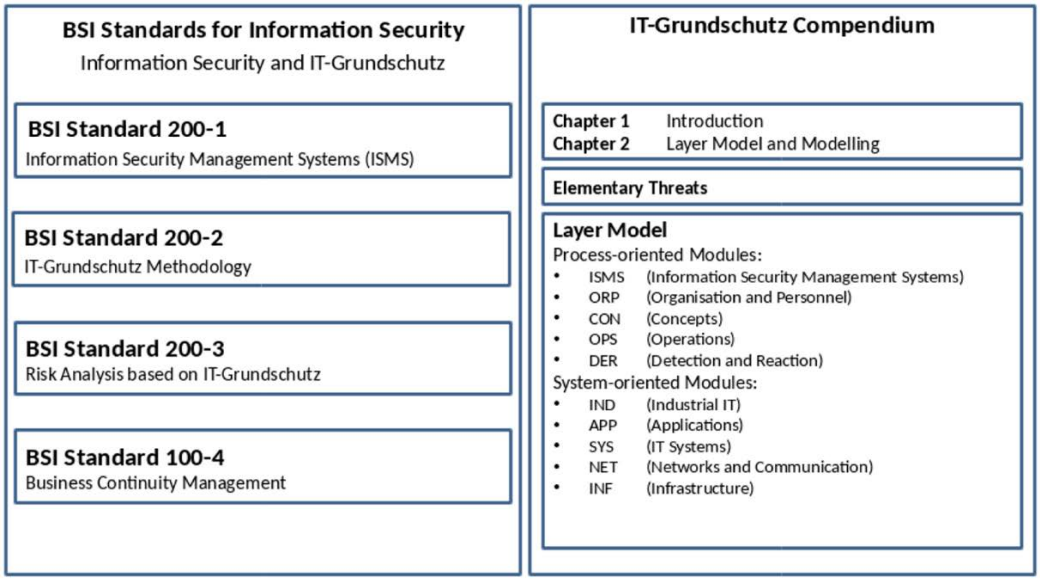


Fig. 6 Current structure of the IT-Grundschutz documents of the BSI [8:185]. Image source: BSI [13:12].

An ISMS comprises all the regulations that help to operate, control, and enhance IS. An ISMS determines which instruments and methods the management of an institution uses to coordinate the necessary tasks and activities in a comprehensible manner (see [8: 181] and [13]). In building up an ISMS, top management must not simply relegate IS to the IT department: it should be a **top priority at management level!**

With the three *BSI standards* and the *IT-Grundschutz Compendium*, ISOs have a good set of instruments at their disposal, as these standards cover all the tasks that they will need to coordinate. In the following chapters, we will examine the IT-Grundschutz approach and the background to it in more detail as a way to optimize use of the modules.

This chapter provides a brief overview of the BSI standards. In addition to the printed edition of the three BSI standards found in the *IT-Grundschutz work manual* [8], all the BSI standards can also be downloaded for free as PDFs from the BSI website [12] and are the basis for an ISO's work. BSI Standard 100-4 (business continuity management) is currently being revised to 200-4 and is equally important for all institutions. This standard is the basis for the work of business continuity officers (BCOs). In our opinion, these two roles—ISO and BCO—should not be filled by one person (see fig. 1 and table 1). The role of the data protection officer (DPO) should also be kept separate. We will come back to this in a later chapter.

BSI Standard 200-1: Information security management systems (ISMS)

BSI Standard 200-1 is completely compatible with the ISO/IEC 27001 standard; it defines the overall requirements for an ISMS and broadly stipulates the safeguards that can be used to initiate, control, and monitor IS in an institution [13]. It explains the four components of an ISMS in a general way (see fig. 7). These four ISMS components are [13:16] as follows:

- management principles (fig. 7, below)
- resources (fig. 7, on the left)
- employees (fig. 7, on the right)
- the security process (fig. 7, above).

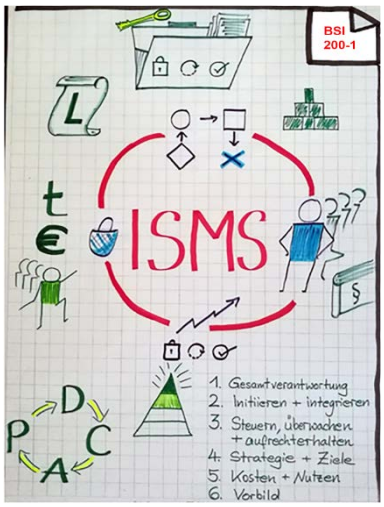


Fig. 7 Flipchart showing the four components of an ISMS as per BSI [13]: management principles (below), resources (left), security process (above), and employees (right).

The *management principles* include the tasks and duties of management (fig. 7, below), regardless of the concrete form an ISMS takes. This involves taking overall responsibility for IS and defining the IS strategy and goals for the institution. In addition, the top management level must initiate, control, and monitor the security process.

Moreover, IS is to be integrated as a cross-sectional function in all the institution's processes and projects within an organization: this includes setting up incident management.

The holistic approach must take into account the difficult trade-off between the costs of the security measures and possible risks and damage.

It is also crucial that managers act as role models. Below is a summary of management's tasks and duties [13:20–22]:

- assumption of overall responsibility for information security
- initiation, management, and supervision of information security
- integration of information security
- setting of realistic objectives
- weighing of security costs against benefits
- role model function.

Monitoring the success of the ISMS and evaluating the entire security process at management level should take place continuously. BSI Standard 200-1 formulates questions for this [13:24f.]. In addition, the necessary, continuous improvement is shown in fig. 5, indicated by the PDCA cycle [3] [4]. PDCA means plan, do, check, and act, as described in this BSI standard [13:18–19].

Resources (see fig. 7, on the left) equate to time and effort, budget and personnel. According to the standard ISO/IEC 27001—and thus also to BSI Standard 200-1—sufficient resources must be made available to the institution's IS by the top management level. BSI Standard 200-1 emphasizes here that IT security is often only associated with technical solutions, and this perspective falls short of the mark. "However, the common belief that security safeguards would inevitably be associated with high levels of investment in security technology and highly specialized security experts is not true. The most important success factors include common sense, properly thought-out organizational regulations, and reliable, well-informed employees implementing the security requirements in an independent and experienced manner. Hence, the costs of developing and implementing an efficient security concept are not necessarily prohibitive, and the most efficient safeguards may prove surprisingly simple." [13:26]. This is confirmed by international research [14] [15].

Employees must be made aware of security issues (fig. 7, right). One key aspect is that IS must be integrated into specific day-to-day activities and tasks. According to BSI Standard 200-1, IS affects all employees without exception [13]. Communication about IS and reporting geared to specific target groups are thus an important aspect of an ISO's work in an institution. "The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security." [13:26].

The *security process* is the real goal of an ISMS (fig. 7, top). According to BSI Standard 200-1, the management level must define the security objectives based not only on the relevant conditions and an analysis of the specific context but also on the objectives of the company or government agency, while creating the prerequisites for their implementation [13:27]. The approach is planned with a security strategy in mind to establish a permanent security process. The strategy is implemented with the help of a security concept and security organization [13:27].

This requires an IS strategy defined by the top management, which is reflected in an IS guideline. It is signed by the management and published internally. Planning the security process involves first determining the appropriate level of security for the business processes, which must be known and modeled (see fig. 1). The scope of the ISMS must then be established. We would recommend starting with a manageable area, called an "information domain." Afterwards, one can gradually expand and develop the institution's security concept. In summary, the security process includes

- an information security policy, in which the security objectives and strategies for their implementation are documented;
- the development of the security concept of the institution, including continuous improvement, because the life cycle of the security concept and all IS processes must be observed; and
- the establishment of a security organization for the institution.

In addition, BSI Standard 200-1 already deals with the *IT-Grundschutz methodology* as a practical example to make clear that it can be used to build an inexpensive ISMS.

BSI Standard 200-2: IT-Grundschutz methodology

We will cover the IT baseline protection (IT-Grundschutz) methodology described in BSI Standard 200-2 in detail with a software-based tutorial (see chapter 3). We will thus confine ourselves to a brief description of it here. The migration guide of the *IT-Grundschutz Compendium* [16] can also be used. In our opinion, the so-called *action points* of BSI Standard 200-2 are of particular practical importance for ISOs [17]. Just on the basis of these action points, the ISOs can clearly specify their areas of responsibility in the overall context. BSI Standard 200-2 thus concretizes BSI Standard 200-1 in the form of a step-by-step procedure.

The phases of the security process according to BSI Standard 200-2 are as follows [17:14]:

- Initiation of the security process
  - Management takes responsibility.
  - The security process is designed and planned.
  - Funding is put in place.
  - An approach is selected.
- Drawing up of an IS policy
- Suitable Organizational Structure
- Drawing up of a security concept
- Implementation of the security concept
- Maintenance and continuous improvement
  - The ISMS is enhanced.
  - The selected approach is extended.

The *individual action points* of BSI Standard 200-2 in the **IS initiation phase** are as follows:

Acceptance of responsibility by management [17:18–19, *3.1*]:

- Management is informed regularly on the possible risks and consequences of a lack of information security.
- Management accepts overall responsibility for information security.
- Management initiates the information security process within the organization and appoints an ISO.

Action points for the **designing and planning of the security process** [17:24–25, *3.2*]:

- Appoint contact persons for all business processes and specialized tasks.
- Perform basic assessment to determine the value and security level of information, business processes, and specialized tasks.
- Delineate conditions governing internal and external framework.
- Gauge the importance of business processes, specialized tasks, and information.
- Set general IS objectives.
- Create a consolidated summary of the present assets based on the knowledge previously gained.
- Secure management agreement.

Action points for **defining the scope of the security concept** [17:27, *3.3.4*]:

- Define which critical business processes, specialized tasks, or parts of the organization should be included.
- Clearly delimit the scope of the concept.
- Describe interfaces with external partners.

Action points for **management decision making** [17:28, *3.3.5*]:

- Elaborate a management template for decision making.
- Decide which approach (basic, core, or standard protection) is to be selected to protect which areas of the organization.
- Document decisions and a schedule for implementation.

Action points for **drawing up an information security policy** [17:30, *3.4*]:

- Issue executive mandate to design a security policy.
- Convene a group to develop the security policy.
- Specify scope and content.
- Organize management approval of security policy.
- Announce the security policy.
- Regularly check and, if necessary, update security policy.

Action points in the **organizational phase of the security process** [17:51, *4*]:

- Stipulate roles for designing the information security process.
- Assign tasks and areas of responsibilities to the roles.
- Stipulate the human resources required for the roles.
- Document the IS organization.
- Integrate information security management into the generic processes.
- Take into account the involvement of external experts.

The concrete structure of the IS organization must be clarified and the tasks, responsibilities, and competencies within this IS organization must be defined. Chapter 4 of BSI Standard 200-2 describes this in detail. The question as to where the ISO or ISOs are anchored organizationally is also important and depends on the size of the institution. BSI Standard 200-2 recommends that the position of the main ISO is assigned directly to the top management level and advises *against* locating the ISO in the IT department, as this can lead to a conflict of roles [17].

In this context, in our opinion, combining the roles of ISO and DSO is not advisable, even if there are thematic overlaps. The DSO's focus and control are directed toward personal data and compliance with the right to informational self-determination (see chapter 5.4), while the ISO wants to ensure the protection of all information and the entire security process. Conflicts can arise here: for example, differing opinions about the scope and extent of logging. BSI Standard 200-2 also problematizes possible conflicts of interest if the tasks of the DSO are transferred to people who already have other roles [17]. We think it is appropriate that within an institution the two functions should be carried out by different people performing a list of tasks at an appropriate skill level, while also working in close cooperation with one another.

Furthermore, in the **organizational phase of the security process**, the documentation before and during the security process becomes relevant. The documentation should be meaningful and comprehensible, while at the same time remaining within an appropriate framework. BSI Standard 200-2 envisages the following action points.

Action point for the **classification of information** [17:46, *5.1*]:

- Create a classification scheme to enable the correct, uncomplicated, and clear classification of information.

The action points on **information flow** in the information security process [17:50, *5.2*]:

- Document basic specifications on information flow and reporting routes for information security process and present this policy to management for approval.
- Inform management of the results of checks and the status of the information security process.
- If required, obtain decisions on the necessary corrective measures.

- Document all sub-aspects of the whole information security process clearly and keep the documentation up to date.
- Assess the quality of the documentation and, if necessary, improve or update it.
- Keep reporting routes that relate to the information security process up to date.
- Find synergies between the information security process and other management processes.

As already mentioned, the updated ("modernized") IT-Grundschutz offers three options in the phase in which a security concept is created (see fig. 2). In this book, we clarify the procedure for ***standard protection***, which is summarized in fig. 8 based on BSI Standard 200-2 [17:63].

The holistic approach of IT-Grundschutz can already be seen in the definition of the scope, because it is based on the business processes, organization, infrastructure, IT structure, and employees involved. We will deal with the individual steps in the process, from structural analysis and the determination of protection requirements and modeling through to the IT-Grundschutz checks 1 and 2—including risk analysis and the implementation of the measures where applicable—with a software-based step-by-step tutorial in chapter 3.

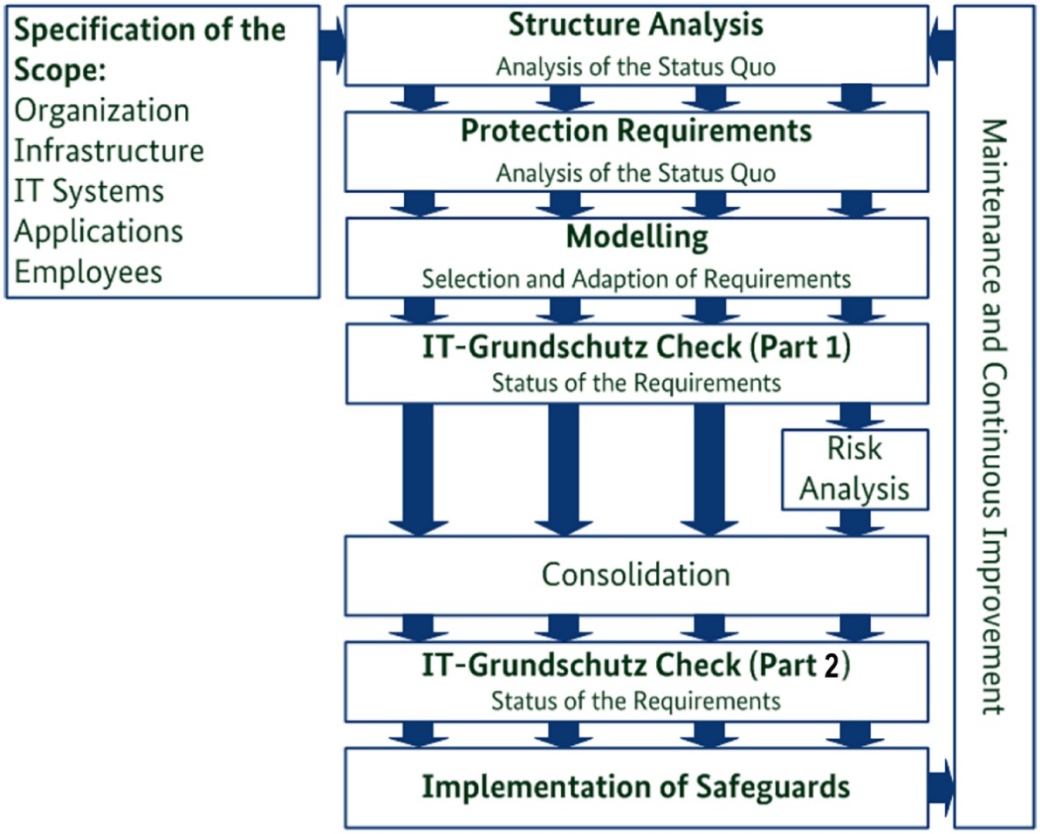


Fig. 8 Drawing up of the security concept for standard protection based on BSI Standard 200-2 [17]: step-by-step creation of the security concept of an information domain. Image source [17:63] improved for part 2.

The individual action points of BSI Standard 200-2 in the **phase of creating a security concept according to the standard protection procedure** are as follows:

Action points for **reducing complexity through the formation of groups** [17:67, *8.1.1*]

- Form groups of similar objects for all sub-tasks in the structural analysis.
- Note the type and number of each of the grouped objects.

Action points for **recording the business processes and related information** [17:68, *8.1.2*]

- Draw up a summary of the business processes.
- Label the business processes with unique numbers or codes.
- Show the correlation between business processes and applications.

Action points for **registering the applications and related information** [17:71, *8.1.3*]

- Find out the applications required for the business processes under consideration by involving the people responsible for the applications and/or their users.
- Draw up a list of the applications and label them with unique numbers or codes.

Action points for **determining a network plan for the information domain** [17:73, *8.1.4*]

- Examine existing graphical depictions of the network—e.g., the network topology plans.
- Update or produce network plans as necessary.
- Examine existing additional information on the IT, ICS, and IoT systems involved and update and improve them as necessary.
- Examine existing additional information on the communication links involved and update and improve them as necessary.

Action points for **listing IT, ICS systems, and other devices** [17:77, *8.1.5*, *8.1.6* and *8.1.7*]

- Check whether existing databases or summaries of the existing or planned IT, ICS systems, and other devices are appropriate as the basis for other procedures.
- Produce or update and improve list of networked and stand-alone IT systems, IoT, and ICS devices.
- Assign IT, ICS, IoT systems or system groups unique names or codes.
- Assign the applications to the IT, ICS, and IoT systems (servers, clients, network switching elements, etc.) required for execution.

Action points for **inventorying the physical space** [17:78, *8.1.8*]

- Produce an inventory of all the properties, buildings, and rooms listed when acquiring the IT, ICS, and IoT systems.
- Add in other rooms in which sensitive information is stored or otherwise processed.

After completing the structural analysis, the institution must specify the protection categories *normal*, *high*, and *very high*, depending on the organization. In order to determine the appropriate protection need categories for the business processes of an institution, supporting applications, IT systems, and communication links, as well as its physical premises, BSI Standard 200-2 [17:79] recommends the use of the following six typical damage scenarios:

- violation of laws, regulations, or contracts
- impairment of the right to informational self-determination
- impairment of the physical integrity of a person
- impairment of the ability to perform tasks
- negative internal or external effects
- financial consequences.

Action points for **defining the protection need categories** [17:82, *8.2.1*]

- Consider typical damage scenarios for defining protection need categories.
- Define "normal," "high," and "very high" protection requirements categories, or adapt them to the individual organization.

Action points for **determining the protection needs for business processes and applications** [17:85, *8.2.3*]

- Define the protection needs of the acquired business processes and applications using the damage scenarios and lists of questions.
- Document the protection needs of the business processes and applications and their corresponding rationales in tables.

Action points for **defining the protection needs for IT, ICS systems, and other devices** [17:89, *8.2.4*, *8.2.5* and *8.2.6*]

- Determine protection needs of the IT, ICS systems, and other devices on the basis of the protection needs of the business processes and applications.
- Consider dependencies, the maximum principle, and, if necessary, cumulative or distribution effects.
- Document the results for confidentiality, integrity, and availability as well as the rationales for each system (group).

Within this procedure, the following **three principles** relating to the three basic values of IS—confidentiality, integrity, and availability—must be considered:

- The *maximum principle* means that the damage or the sum of the damage with the most serious effects determines the protection needs of, for example, an IT system [see 17:85].

- The *cumulative effect*, on the other hand, means that processing several applications with smaller levels of individual damage on one IT system can cause a higher level of damage overall [see 17:86].

- The *distribution effect* is the opposite effect and can occur if, for example, only insignificant parts of an application run on one IT system, so that the application's high need for protection is not transferred to the system, particularly if corresponding safeguards are implemented [see 17:86].

Parallel considerations must also be taken into account in the action points for **defining the protection needs for physical spaces** [17:90, *8.2.7*]:

- Infer the protection needs of the physical spaces from the protection needs of the business processes, applications and IT systems, ICS, and other devices.
- Consider dependencies, the maximum principle, and, if necessary, the cumulative effect.
- Document results and rationales clearly.

Action points for defining the **protection needs for communication links** [17:92, *8.2.8*]

- Acquire external connections and document them in tabular or diagrammatic form.
- Identify connections that are used to transfer critical information.
- Document all critical communication links in tabular or diagrammatic form.

The action points for **conclusions** drawn from the results of the protection needs assessment [17:94, *8.2.9*] complete this documentation:

- Check whether objects with increased security requirements can be concentrated in secure zones.
- Earmark objects with increased security requirements for risk analysis.

The structural analysis and determination of specific protection needs provide all the necessary data for the information domain in question. The next step is the so-called *modeling* of the information domain (see fig. 8). IT-Grundschutz protection involves selecting the necessary modules and making decisions on the measures required. The elementary threats are also referenced in the individual IT-Grundschutz modules. These constitute the first stage in a simplified risk analysis for typical information processing environments in order to ensure an appropriate level of IS for the institution.

As BSI Standard 200-2 says, "This list of threats is part of the first level of the simplified risk analysis for typical environments of information processing and represents the basis on which the BSI compiled specific requirements for ensuring an appropriate level of information security in an organization. The advantage of this is that the users are not required to use costly or further analyses for typical application cases in order to achieve the security level required for normal protection needs. Instead, it is sufficient to identify the modules relevant for the business processes under consideration and their required resources, and to rigorously and completely fulfil the requirements recommended there." [17:95].

Action points for **modeling an information domain** [17:104, *8.3*]

- Work through the Section Layer model and modeling in the *IT-Grundschutz Compendium* systematically.
- Determine the target objects in the information domain under review to which each module in the *IT-Grundschutz Compendium* is to be applied.
- Document the assignment of modules to target objects ("IT-Grundschutz model") and the relevant contact people.
- Note target objects for a risk analysis that cannot be modeled appropriately.
- Determine an order for implementing the modules.
- Carefully read the security requirements of the identified modules and determine relevant security safeguards on this basis.

The next step is the so-called *IT-Grundschutz check (1)*, a target-performance comparison, which consists of the following action points:

Action points for the **organizational preliminary work for the IT-Grundschutz check** [17:106, *8.4.1*]

- Examine internal documents to identify responsibilities and rules and clarify who is responsible for these documents.
- Determine to what extent external assistance is required.
- Stipulate main contact person for all the modules used in the modeling.
- Agree appointments for interviews.
- Assemble team for interviews.

Action points for carrying out the target-performance comparison and **performing gap analysis** [17: 107, *8.4.2*]

- Prepare checklists in advance for each specialized area.
- Explain the objective of the IT-Grundschutz check to the interview partners.
- Ask for the implementation status of the individual requirements.
- Verify answers using samples in situ.
- Inform the interviewee of the results.

Action points for the **documentation of the results** [17:108, *8.4.3*]

- Acquire master information for every target object.
- Document information on the IT-Grundschutz check and its implementation status.
- Include fields or placeholders for implementation planning.

This is followed in BSI Standard 200-2 procedure by the treatment of risk analysis, which is summarized as a complete process (risk management) and detailed in BSI Standard 200-3 on the basis of IT-Grundschutz. However, a risk assessment for areas with *normal* protection needs and typical hazards is *implicitly* carried out when the IT-Grundschutz modules are applied.

With the modeling and use of the implementation instructions of the IT-Grundschutz, this implicit risk assessment is included in the security concept of an information domain. The advantage for users of IT-Grundschutz is that they do not have to carry out any further individual threat and vulnerability analysis for a large part of the information domain [see 17:109]. However, such an explicit risk analysis must be carried out, for example, if the information domain contains target objects that

- have high or very high protection needs in at least one of the three basic areas of confidentiality, integrity, or availability, or
- cannot be adequately modeled with the existing IT-Grundschutz modules, or
- are operated in application scenarios that are not provided for in the context of IT-Grundschutz [17:109].

In practice, the question often arises as to whether such an explicit and complex risk analysis should be carried out immediately after the IT-Grundschutz check (part 1; see fig. 8) or only after the full implementation of security measures for *normal* protection. BSI Standard 200-2 summarizes the advantages and disadvantages of these alternative sequences [17:111]. Ultimately, this must be decided by each institution according to its overall framework, security risk management, and the type of information domain selected. The ISO once again has the role of central communication and coordination. Moreover, the institution is free to use another established method—outside of BSI Standard 200-3—for the analysis of information risks.

BSI Standard 200-2 describes the following action points for **risk analysis** [17:111, *8.5*]:

- Document the basic procedure of the organization for the performance of risk analyses and present this policy to management for approval.
- Determine the target objects or groups of target objects for which a risk analysis should be performed.
- Systematically work through BSI Standard 200-3 risk analysis based on IT-Grundschutz.
- Integrate the results of the risk analyses into the security concept.

According to fig. 8, the implementation of the selected security measures still needs to be planned, carried out, supervised, and monitored. It should be noted that only limited resources are available for the implementation of the measures in the institution, so that it is important to choose the most efficient means of implementation.

There are often different ways to meet the security requirements with suitable technical-organizational measures (TOM). However, implementation instructions with practical recommendations are already in place for the IT-Grundschutz modules. In any case, management must be kept informed of the outcomes of the security investigation and make relevant decisions regarding safety requirements and the TOM and its alternatives.

ISOs usually have to raise awareness at the management level. To do this, they can list security needs and requirements that have not been met or where deficiencies have been noted, identify specific threats from the IT-Grundschutz modules, or use the *cross-reference tables*. These provide an overview for each IT-Grundschutz module, including information about which requirements work against which elementary threats, making it possible for residual risks to be listed [see 17:114]. “The residual risk relating to any chance or wilful threats should be described clearly and presented to the management level for a decision. The remaining steps can only occur after management has decided that the residual risk is acceptable, as they must bear responsibility for the consequences.” [17:114].

The management must decide on the budget for the measures. After that, the order of implementation must be determined and a binding decision made about who will implement which measures by when and report on them after completion. Typically, the implementation work will be reported to the ISO as the central coordination point. According to BSI Standard 200-2, ISOs must be continuously informed about the progress and results of implementation. They regularly inform management about the associated reduction in existing risks. The implementation plan should contain the following information at a minimum [17-116]:

- description of the target object as operational environment
- number and/or title of the module in question
- title and/or description of the requirement to be fulfilled
- description of the safeguard to be implemented and/or reference to the description in the security concept
- implementation scheduling, budget planning—e.g., for provisioning and operating costs of components
- persons responsible for implementation of the safeguards.

Action points for **implementing the security concept** [17-117, *9*]

- Summarize missing or only partially implemented IT-Grundschutz requirements as well as additional security safeguards in a table.
- Consolidate security safeguards—i.e., delete unnecessary safeguards, adapt general safeguards to the particular situation, and check all safeguards for suitability.
- Determine one-off and repeat costs and expenses for the safeguards that are to be implemented.
- Determine replacement safeguards for those that cannot be financed or provided.
- Take decisions on which resources are to be used to implement the safeguards.
- If necessary, highlight residual risk and obtain decision on this from management.

- Specify, provide rationale for, and document order in which safeguards are to be implemented.
- Stipulate implementation deadlines and assign responsibilities.
- Monitor implementation and adherence to deadlines.
- Train and raise awareness of affected employees.

It is still necessary thereafter to ensure the maintenance and continuous improvement of an institution's IS: to achieve this, a success control and evaluation of the IS process should take place at management level. For this purpose, ISOs must clearly sample the relevant information. The effectiveness of an institution's ISMS can be assessed using (well-chosen) key figures or a so-called maturity model. In addition, after the introduction of new security measures, the ISO should check whether there is the necessary acceptance of them among employees. The causes of any lack of acceptance must be worked out and eliminated as per BSI Standard 200-2. For this purpose, awareness and training concepts need to be designed, implemented, and evaluated (see chapter 4). Overall, "the task of the ISO is to collect and process such information and to edit [it] for the management level in a brief and clear manner." [17: 118].

It is also important that the information security strategy should make key statements on measuring the achievement of objectives. At the very least, according to BSI Standard 200-2, it is necessary to define [17:118]

- which objectives are monitored or measured in which form (WHAT),
- who is responsible for monitoring or measuring the items previously specified (WHO), and
- when and how often the results are to be evaluated (WHEN).

A maturity model can help to clearly document the temporal development of the institutional ISMS without providing too many details about individual protective measures. BSI Standard 200-2 contains the following maturity assessment of an ISMS [17: 119]:

- Maturity level 0: There is no ISMS and there are no plans for establishing an ISMS.
- Maturity level 1: An ISMS is planned but not established.
- Maturity level 2: An ISMS is partially established.
- Maturity level 3: An ISMS is fully established and documented.
- Maturity level 4: In addition to maturity level 3, the ISMS is checked regularly for effectiveness.
- Maturity level 5: In addition to maturity level 4, the ISMS is improved on a regular basis.

However, it should be noted that the assessment of the maturity level of an ISMS can be multidimensional and quite complex if all the aspects are considered, based on the layer model of the *IT-Grundschutz Compendium* (see fig. 6).

According to BSI Standard 200-2, the relevant action points for **maintaining and continuously improving information security** are as follows [17:123, *10*]:

- Record the organization's basic approach to checking and improving the information security process in a policy document and present this to management for approval.
- Integrate measurement of the degree to which objectives have been achieved into the security strategy.
- Check adherence to the implementation plan.
- Check implementation of the safeguards agreed.
- Check the effectiveness and efficiency of the safeguards agreed.
- Check whether the security safeguards have been accepted, and improve if necessary.
- Consider any conflict of roles between creator and auditor.
- Ensure confidentiality of the examination results.
- Check suitability and currency of security objectives, strategies, and concept.
- Check appropriateness of resources provided and the cost-effectiveness of the security strategy and security safeguards.
- Allow the results of checks to flow into improvements in the information security process.

If an institution is looking for certification, the action points on **ISO 27001 certification based on IT-Grundschutz** are as follows [17:124-125, *11*]:

- Read information on the scheme for ISO 27001 certification on the basis of IT-Grundschutz.
- Check whether work regarding information security should be made transparent by means of an ISO 27001 certificate on the basis of IT-Grundschutz.
- If necessary, check whether the information security management and the security status meet the relevant requirements.
- If necessary, initiate the certification process.

BSI Standard 200-3: Risk analysis based on IT-Grundschutz

The risk analysis based on IT-Grundschutz as specified by BSI Standard 200-3 covers all risk management—i.e., the entire process of identifying, assessing, evaluating, and addressing risks. According to the relevant literature and international ISO/IEC 27005 standard, the term *risk analysis* usually denotes just one step in the context of risk management. Fig. 9 shows a general outline of the process loop for risk management. Its components are risk identification, risk assessment, risk analysis, risk treatment, and risk documentation.

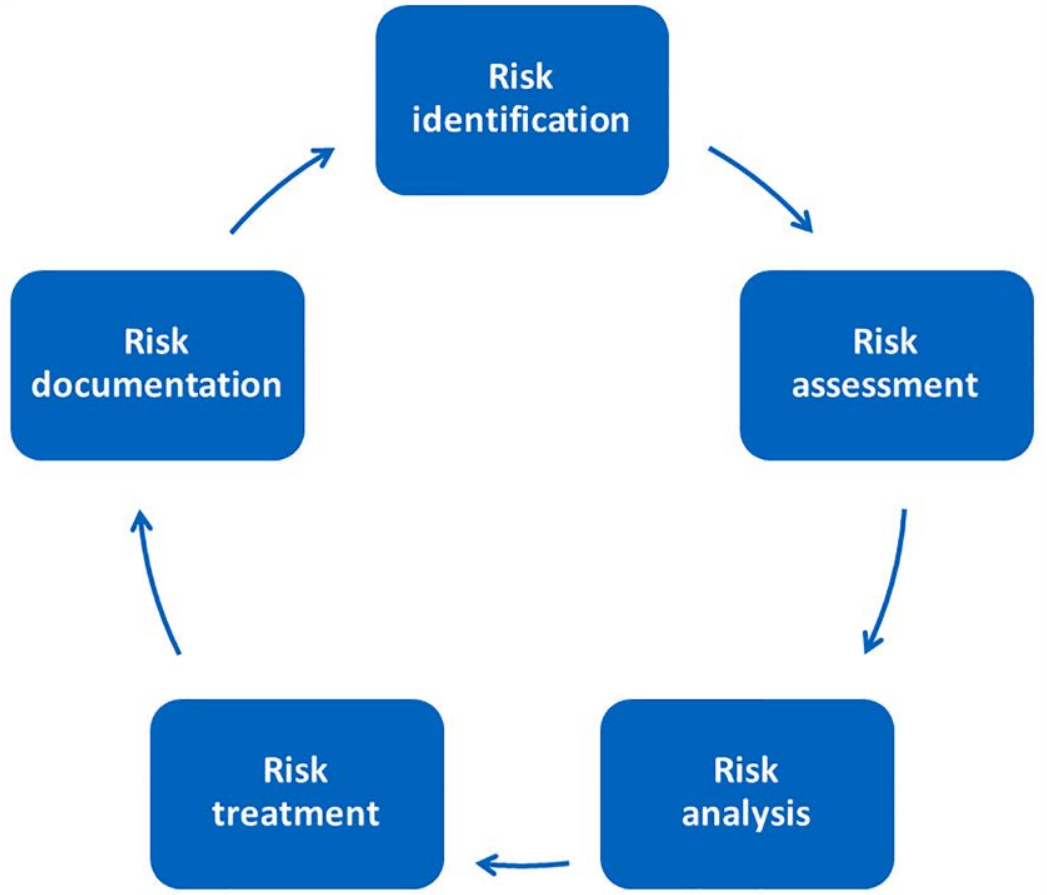


Fig. 9 General process outline for risk management.

Since risks change over time or may arise from a change in tasks, risk management must be constantly reviewed.

According to BSI Standard 200-3 [18:6], the **first step** involves risk identification through examination of the forty-seven elementary threats summarized in the standard or *IT-Grundschutz Compendium* (see fig. 6 and table 2). If necessary, additional threats need to be identified that may arise from the institution's specific business process and operational scenario. In particular, the BSI's elaboration and description of the elementary threats based on IT-Grundschutz should lead to the efficient implementation of risk management with regard to the three basic values of IS. In order to ensure confidentiality, integrity, and availability, the BSI shows which basic value is directly affected by which elementary threat, as indicated in table 2 (right column). The **second step** based on BSI Standard 200-3 [18:6-7] is to undertake risk classification, which consists of two components: risk assessment and risk evaluation. Risk assessment means determining the frequency of occurrence and the extent of any damage. Risk evaluation means determining the risk category. In distinction to fig. 9, this is a summary of the risk assessment and actual risk analysis. In the new German standard version of ISO/IEC 27005, risk identification, risk assessment, and risk analysis are jointly referred to as risk judgment [11:41]. So, the terminology for risk management is not really consistent.

Elementary threats according to BSI IT-Grundschutz		Core values
G 0.1	Fire	A
G 0.2	Unfavorable 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	Unauthorized 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	Unauthorized 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 authorizations	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 actions	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	Unauthorized 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

Tab. 2 Overview of the elementary threats with the relevant affected core values of BSI Standard 200-3 [18:12]. The main values affected in the right column are abbreviated to the English terms: C for confidentiality, I for integrity, and A for availability.

In general, risks have two sides to them, relating to cause, usually connected with a probability of occurrence, and damage, the extent of which needs to be assessed. On the causal side, the measures used should ultimately lead to the avoidance of such causes. Measures used on the damage side should lead to a reduction in the negative effects of such damage. These two sides form the so-called risk matrix, which the updated BSI Standard 200-3 has now adopted in four stages (see fig. 10). The task of the institution is therefore to specify the categories of occurrence frequency *rarely*, *medium*, *frequently* (called *"often"* in fig. 10), and *very frequently* (called *"very often"* in fig. 10) for the causes. The BSI standard makes suggestions for this [18:21]. Likewise, the damage categories need to be defined for the institution and the operational scenario: *negligible*, *limited*, *significant*, and *life-threatening* (i.e., threatening the existence of the organization). However, the explanations for the damage categories given in the standard are too general (see [18:21-22]).

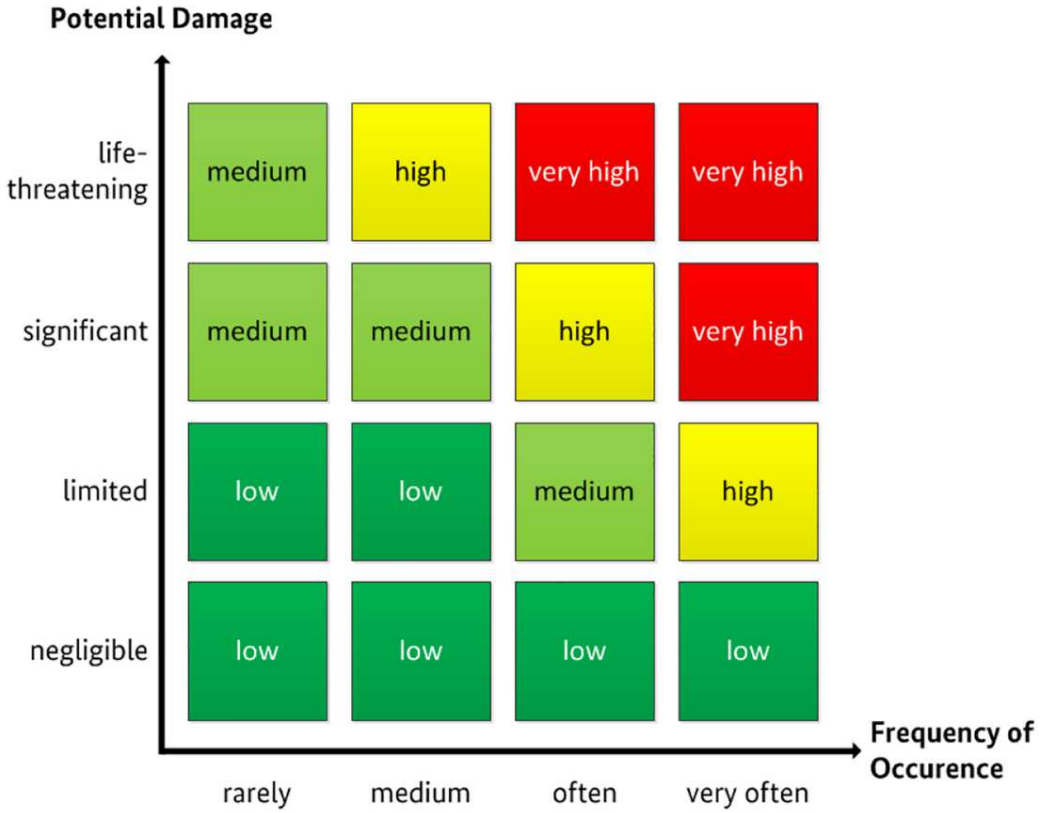


Fig. 10 Matrix for classifying risks as per BSI Standard 200-3 [18:22].

The risk categories specifed in BSI Standard 200-3 [18:22] (see fig. 10) have the following meaning:

- *Low*: The security measures implemented or envisaged in the security concept offer sufficient protection and can therefore be accepted in practice, although these threats should still be monitored.
- *Medium*: The security safeguards already implemented or at least envisaged might not be sufficient.

- *High*: The security measures implemented or envisaged do not provide adequate protection against a particular threat.
- *Very high*: The security safeguards implemented or envisaged in the security concept do not provide adequate protection against a particular threat and cannot be accepted in practice.

The **third step** of the IT-Grundschutz risk analysis is *risk treatment* [18:7], for which the following four strategies are listed in BSI Standard 200-3 [18:27]:

- Risk avoidance—if the cause of the risk is excluded
- Risk reduction—using security measures that qualify the classification (reduce the risk catagories)
- Risk transfer—transferring risks to other parties
- Risk acceptance—if the risks can be lived with and there are opportunities to be grasped.

The BSI standard emphasizes that the next step in this risk treatment strategy differs considerably from organization to organization [18:22], and no general recommendation can be made for all institutions. The strategy must take into account many individual aspects of the institution as a whole, and the institution has to make specific decisions. Management will have different risk preferences and a different level of risk acceptance. BSI Standard 200-3 speaks of “risk appetite” within the individual organization [18:23]. Chapter 6 of the standard covers the risk treatment options by asking a number of questions, and chapter 9 explains them using various practical examples.

The final step, according to fig. 9, is *risk documentation*. This **fourth step** according to IT-Grundschutz involves the consolidation of the security concept (see also fig. 8). In practice, this is usually the integration of additional safeguards in the security concept. Based on the risk management, the security measures for each target object in the information network are checked based on the following criteria:

- Suitability of the security measures to prevent threats
- Interaction of security measures
- Ease of use of security measures
- Appropriateness and quality assurance of the security measures
- Integration into the existing security concept of the requirements ascertained from risk management.

After applying this procedure based on BSI Standard 200-3, we can return to BSI Standard 200-2 and continue the IT-Grundschutz methodology (see fig. 8):

- IT baseline protection check (IT-Grundschutz check part 2)
- Implementation of all safeguards within the security concept
- Review of IS process at all levels and flow of information in the entire IS process
- ISO 27001 certification (where applicable) based on IT-Grundschutz.

It should be noted that the BSI provides an online course (in German only) on information security, in which every step of the IT-Grundschutz training is explained [19]. Lesson 7.7 [19] is part of the subject matter discussed here.

BSI Standard 100-4

BSI Standard 100-4 for business continuity management, which has not yet been completely updated, is described in chapter 6 of this book.

Implementation and training exercises

ISOs in Germany, especially in public administrations, must know and understand the BSI standards. The many practical tips and explanatory examples can also be a great help for ISOs in other countries. Therefore, appropriate further training should enable participants to work actively with these standards. BSI Standards 200-x should be worked through by participants to enable them to exchange implementation ideas. This means that there are questions or prompts that require participants to read the BSI standards in more detail to answer them.

Examples of questions for **BSI Standard 200-1**:

- Explain the four components of an ISMS.
- What are the tasks and duties of the top management when setting up an ISMS?
- What does “management responsibility” mean in the security process?
- What should the exchange of information and reporting look like?
- Give reasons why security should be an integral part of planning, designing, and operating business processes and information processing.
- List the most important success factors crucial to building an ISMS.
- Why is it often difficult in practice to establish an appropriate and adequate level of security and to maintain it over the long term?
- What is an institution’s IS guideline? What does IS revision mean?
- How can a security level, once it has been achieved, be maintained and improved over the long term?
- Can you give a brief explanation of BSI Standard 200-1 to your management?
- Can you explain the life cycle of the security concept to your management?

With regard to **BSI Standard 200-2**, ISOs should be able, at a minimum, to deal with the following questions or requests for clarification:

- What does BSI Standard 200-2 actually represent?
- What is the structure of the information security organization in your institution?

- What is the ideal structure of the information security organization for a large institution? What adjustments in the ideal structure of the information security organization should be made for a medium-sized or a small institution?

The six damage scenarios specified—along with explanations—in the appendix to BSI Standard 200-2 can be optimally used for an awareness-raising exercise. We created the scenarios in the form of cards along with some examples (see example in German in fig. 11, top). Likewise, the three basic IS values are indicated on the cards using symbols. The three categories covering the possible protection needs are also shown on the cards, which are assigned with magnets on a board (see fig. 11, bottom). First, all six damage scenarios are discussed and attached to the board. The selected examples are then distributed to the participants with the request that they read the particular example out loud, before deciding which damage scenario it can be assigned to—followed by an explanation of their decision. Once all the examples have been assigned, participants discuss which particular basic value is primarily involved.

Fig. 11 The appendix of BSI Standard 200-2 as a card set for an experience-oriented learning scenario geared to the game-based learning (GBL) method (here in German, although you can create something similar with the English version of the standard).

Fig. 12 An intermediate result of the experience-oriented learning scenario for BSI Standard 200-2 produced by participants in an ISO training course (here in German, although you can create something similar with the English version of the standard).

The participants receive the cards with the three basic IS values and should assign them to the different examples while justifying their choices (see fig. 12). Ultimately, the participants understand in a playful way that, according to IT-Grundschutz, all the target objects in the information domain must be checked for these three basic values. The last phase in the experience-based learning scenario is the discussion and assignment of the protection needs categories. Here, too, the exchange of experience between the participants is an important element of awareness raising, because at the beginning the categories *high* and *very high* are often assigned too thoughtlessly. A look at BSI Standard 200-2 leads to the internal definition of the three protection requirement categories. This discussion can best clarify the original importance of IT-Grundschutz as a means to secure a *(normal) standard level* of protection. With regard to the modernization of IT-Grundschutz, the discussion also expands the focus on the lower basic security level and on higher levels of risk (core security protection).

Since the IS guideline is a central document in the security process, and the top management of an institution needs to express to employees the importance of IS, intensive exercises are a useful way to convey the level to be striven for and the mandatory principles of IS. Such guidelines for IS must deal with the specific structure and scope of the institution by posing a variety of questions, which can be used as part of the training. Moreover, there are many public examples of specific guidelines on the World Wide Web (WWW). According to BSI Standard 200-2, the institution's trained IS management team is responsible for the development, review, and revision of such a security guideline [17]. An ISO coordinates the draft guidelines and submits them to the top management of an institution for approval. The final version officially comes into force when the top management approves it.

Questions in the exercise to guide participants in creating an IS policy for their institution might include the following:

- What is an IS policy according to BSI Standard 200-2?
- What is the IS policy in your institution (scope, content)?
- What is the level of awareness vis-à-vis the IS policy in your institution?
- How easily can you find your institution's policy?
- How often and why should an IS policy be reviewed and improved?
- Suppose your institution has had an IS policy for years. What changes should be made to an existing policy if its scope is to be extended to the use of mobile IT systems?
- What does the definition section of an IS policy contain, and what is found in the analysis and regulatory sections?
- Why should the policy of an institution be officially reaffirmed after a change? And what does this mean in practice?
- BSI Standard 200-2 speaks of the establishment of a *development group* to help generate the security guideline if the ISM is just being set up and no IS team exists.

- Who should be a member of this kind of development group, and who specifically would that be in your institution?

For BSI Standard 200-3, we have designed the following interactive exercise for participants (fig. 13): on the board, a risk matrix is drawn with the four categories for each of the two dimensions (damage and frequency of occurrence). All the people involved agree on a specific information domain for the exercise. The total of forty-seven elementary threats are noted on cards, and these are distributed in full or as a selection to all participants. One person begins by reading a threat out loud. Afterwards, the group discusses where this threat should be located in the matrix, and the card is then put there. This procedure is repeated for all the BSI Standard 200-3 elementary threats that have been distributed, so that each of the participants is actively involved as well. Our experience shows that the moderator in the discussion between the participants should refer to the descriptions defined in the standard [18]. For example, in assessing the amount of damage, the four categories are *negligible*, *limited*, *significant/considerable*, and *threatening the existence of the organization*, whereby the difference between *limited* and *considerable* is a matter of some controversy. BSI Standard 200-3 [18] defines the frequency of occurrence as follows:

- *Rarely* (the event could occur every five years at most)
- *Medium* (the event occurs once every five 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).

In the next step, participants can discuss additional threats. In our experience, there are very few additions.

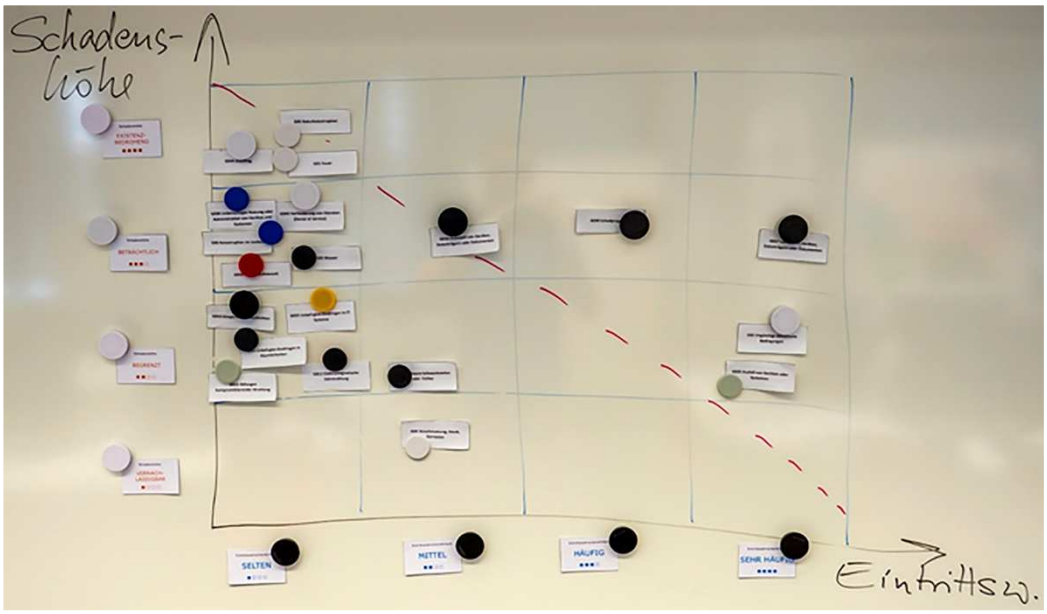


Fig. 13 An intermediate result for the exercise risk matrix using the elementary threats as per BSI Standard 200-3 and a selected defined information domain (here in German, although you can create something similar with the English version of the standard).

Test yourself with the following questions and comments on chapter 2.2:

- What roles do you need for the design of the information security process, and what tasks and areas of responsibility can be assigned to these roles?
- How should the reporting system for the IS process be structured?
- Name the sequence of steps for the *standard* protection of IT-Grundschutz.
- What does *basic* protection in the updated ("modernized") IT-Grundschutz mean?
- What does *core* security in the updated IT-Grundschutz mean?
- What needs to be specifically defined and by whom during the structural analysis?
- What does the "normal" protection need category mean according to IT-Grundschutz?
- What do the protection need categories "high" or "very high" mean and what are the consequences?
- What tasks are to be done specifically, and by whom, when determining protection needs?
- What does the term modeling mean in the IT-Grundschutz approach?
- What is actually done in an IT-Grundschutz check?
- What does gradual implementation of the security concept in IT-Grundschutz mean?

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

2.3 The BSI *IT-Grundschutz Compendium*

According to the BSI, the *IT-Grundschutz Compendium* is the key IT-Grundschutz publication, which, together with the BSI standards, deals extensively with the topic of IS [20]. As shown in fig. 6, the compendium consists primarily of the IT-Grundschutz modules, which in turn deal with a specific security topic and its requirements in context. All IT-Grundschutz modules have a uniform structure: first, the relevant threats to the security topic are explained, and then the important security requirements are broken down into basic, standard, and core security for an institution.

The total of ten IT-Grundschutz modules are divided into the two categories *process* and *system* modules according to fig. 6. The BSI also speaks of the division into ten different layers, which range thematically from applications (APP) through industrial IT (IND) to security management (ISMS) [20]. The *IT-Grundschutz Compendium* is continuously updated. It is published in a new edition every February and can be downloaded as a PDF from the BSI website.

In addition to the IT-Grundschutz modules, suitable implementation instructions are also published (in German), which describe in detail how the requirements of the modules are met and how individual measures can be implemented. Proper implementation instructions do not as yet exist for all the modernized modules. Further implementation information will be added and published. The modules already include a risk assessment for areas with "*normal" (standard) protection needs*, and their requirements reflect the current state of the art.

In the following chapters of this book, we will repeatedly refer to these IT-Grundschutz components and the implementation instructions of the *IT-Grundschutz Compendium* when dealing with the individual security concept and security issues. At this point, we would like to show just one example that fits directly within the previous chapters: the *ISMS Security Management process module* [21] and its implementation notes (still in the 2019 edition and in German) [22]. This deals with the following content [22]:

1 Description
- 1.1 Introduction
- 1.2 Objective
- 1.3 Delimitation and modeling

2 Threat situation
- 2.1 Lack of personal responsibility in the security process
- 2.2 Lack of management support
- 2.3 Inadequate strategic and conceptual requirements
- 2.4 Inadequate or misguided investments
- 2.5 Inadequate enforceability of security measures and guidelines
- 2.6 Failure to update the security process

We can connect the following requirements with fig. 1 and table 1. ***Basic protection*** yields the following requirements, which **MUST** be prioritized for security management [22] [23]:

- ISMS.1.A1 Assumption of overall responsibility for IS by the management level [institutional management] (B)
- ISMS.1.A2 Definition of security goals and strategy [institutional management] (B)
- ISMS.1.A3 Creation of a policy on information security [institutional management] (B); in practice, this is often delegated to the ISO, but adoption of the policy must be the responsibility of the top management of an institution
- ISMS.1.A4 Appointment of an information security officer [institutional management] (B)
- ISMS.1.A5 Drafting of contract when appointing an external ISO [institutional management] (B)
- ISMS.1.A6 Establishment of a suitable organizational structure for IS [institutional management] (B)
- ISMS.1.A7 Definition of security measures (B)
- ISMS.1.A8 Integration of employees in the security process [line manager] (B)
- ISMS.1.A9 Integration of information security in organizational procedures and processes [institutional management] (B).

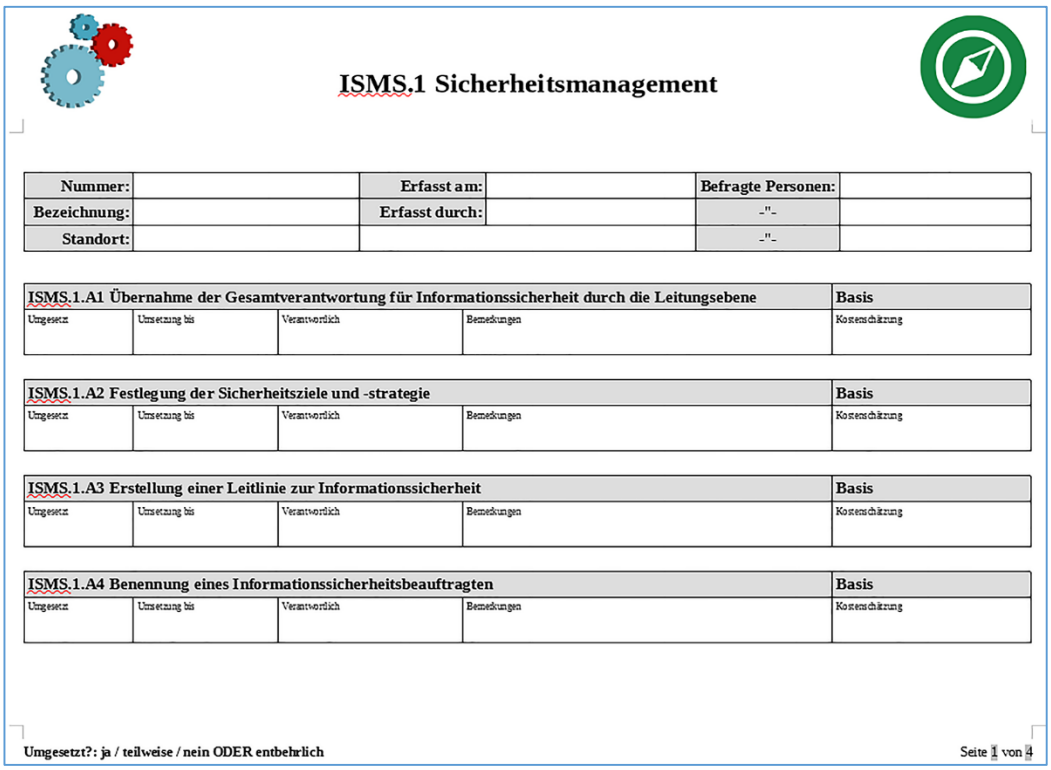
Together with these basic protection requirements, the following additional requirements apply to the ***standard protection*** and **SHOULD** be implemented in line with IT-Grundschutz [22] [23] (see also fig. 1 and table 1):

- ISMS.1.A10 Creation of a security concept (S)
- ISMS.1.A11 Maintenance of information security (S)
- ISMS.1.A12 Management reports on information security [institutional management] (S)
- ISMS.1.A13 Documentation of the security process (S)
- ISMS.1.A14 Awareness raising on information security (S)
- ISMS.1.A15 Economic use of resources for information security (S).

We would like to note that an institution should, in principle, apply all of the IT-Grundschutz modules relevant to the specific situation. To facilitate a seamless implementation sequence, the BSI has marked all modules with *R1*, *R2*, or *R3*. Ultimately it is up to the institution itself which order it chooses. However, the BSI gives the following recommendations to indicate the significance of **Rx** [23]:

- **R1** modules should be implemented primarily because they form the basis of an effective security process.
- **R2** modules should be implemented next, as they are essential for sustainable security in key parts of the information domain.
- **R3** modules must also be implemented in order to achieve the desired level of security. However, it is recommended that they are looked at one by one.

We can also recommend another work produced by the BSI: the checklist manual containing all the test questions from the *IT-Grundschutz Compendium* relating to the effectiveness of an established ISMS [24]. As Holger Schmidt from the BSI wrote in the preface to the checklist manual, it is based "on the requirements that are described in the modules in the *IT-Grundschutz Compendium*. The checklists are a helpful addition for all users who want to use IT-Grundschutz to get a realistic view of the status quo of information security in their institution. The test aspects can be used to understand how high the level of information security is in individual processes or systems, or where there is a need for action." [24].



ISMS.1 Sicherheitsmanagement

Nummer:		**Erfasst am:**		**Befragte Personen:**	
Bezeichnung:		**Erfasst durch:**		-"-	
Standort:				-"-	

ISMS.1.A1 Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene				**Basis**
Umgesetzt	Umsetzung bis	Verantwortlich	Bemerkungen	Kostenschätzung

ISMS.1.A2 Festlegung der Sicherheitsziele und -strategie				**Basis**
Umgesetzt	Umsetzung bis	Verantwortlich	Bemerkungen	Kostenschätzung

ISMS.1.A3 Erstellung einer Leitlinie zur Informationssicherheit				**Basis**
Umgesetzt	Umsetzung bis	Verantwortlich	Bemerkungen	Kostenschätzung

ISMS.1.A4 Benennung eines Informationssicherheitsbeauftragten				**Basis**
Umgesetzt	Umsetzung bis	Verantwortlich	Bemerkungen	Kostenschätzung

Umgesetzt?: ja / teilweise / nein ODER entbehrlich Seite 1 von 4

Fig. 14 Example of a BSI checklist for the ISMS module (page 1 of 4 in German) [25]. An important aspect here is how the implementation is carried out. The categories are "yes," "partially," "no," or "unnecessary."

The checklists (currently in the 2019 edition, in German and without explanations) can be downloaded as electronic files from the BSI website [25]. For the *ISMS module* explained above, the first page of this checklist from [25] is shown in fig. 14. These checklists are useful templates for the ISO and make their coordination, communication, and recording work much easier. If the institution is striving for certification of its ISMS, these checklists are an indispensable internal orientation before the actual inspection by the external auditors of a certification body begins.

Implementation and training exercises

The compendium is very extensive. That is why only selected examples of practical exercises are available. The checklists prove to be a very helpful tool for discussing the requirements and practicing the procedure with participants.

We present a concrete tool-based exercise in the next chapter.

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

3 Tool-supported development of a security concept based on the IT-Grundschutz approach to standard protection

3.1 Preparing and defining the scope (information domain)

As already noted in the introduction, we will use the standard protection approach in this chapter to demonstrate the tool-based development of a security concept. For all German authorities covered by the Federal Implementation Plan (UP Bund), this standard protection is a minimum requirement and is to be coordinated by the ISOs. For all institutions that strive for an ISO/IEC 27001 certification based on IT-Grundschutz, the standard protection approach is also mandatory, because certification only applies to this and to the core protection approach. With the basic protection approach, an ISO/IEC 27001 certificate cannot be obtained. Regardless of whether the institution is striving for such a certification or not, the first step is to determine the field of application for which the IS concept is to be developed. In line with the IT-Grundschutz terminology, this is called the *information domain*. We have already pointed out that the information domain does not necessarily have to encompass the entire institution from the start. Instead, you can start with a reasonably delimited, sufficiently large section and then gradually expand it.

According to BSI Standard 200-2 [17], all the infrastructural, organizational, personnel, and technical components that serve to fulfill business tasks and information processing in a particular area must be taken into account when specifying the information domain for the security concept that is being drawn up (see fig. 8, left). This may include certain organizational units within an institution [17:63], although it can also relate to specific business process and tasks and the infrastructure needed to support them. The components covered by the *IT-Grundschutz Compendium* are part of the relevant information domain [17:63]. For the standard protection approach, the organizational structure involving the business processes, the infrastructure, the IT systems, the software applications, and the employees and other users must be taken into account as part of the information domain (see fig. 1 and table 1). Developing the security concept means that the defined field of application is to be safeguarded by IS measures in accordance with the associated modules from the *IT-Grundschutz Compendium* [22] [23] [24] [25]. Before the security concept can be drawn up, the information about the business processes, support, network plans, interfaces, etc., must be available and up to date.

Implementation and training exercises

The concrete steps for drawing up a security concept based on the IT-Grundschutz approach are explained in the following sections using a brief example selected from the Research Group Scholl (in German, “Forschungsgruppe Scholl” or FS). So far, we have only used this exercise in our German-language training courses and in university classes taught exclusively in German.

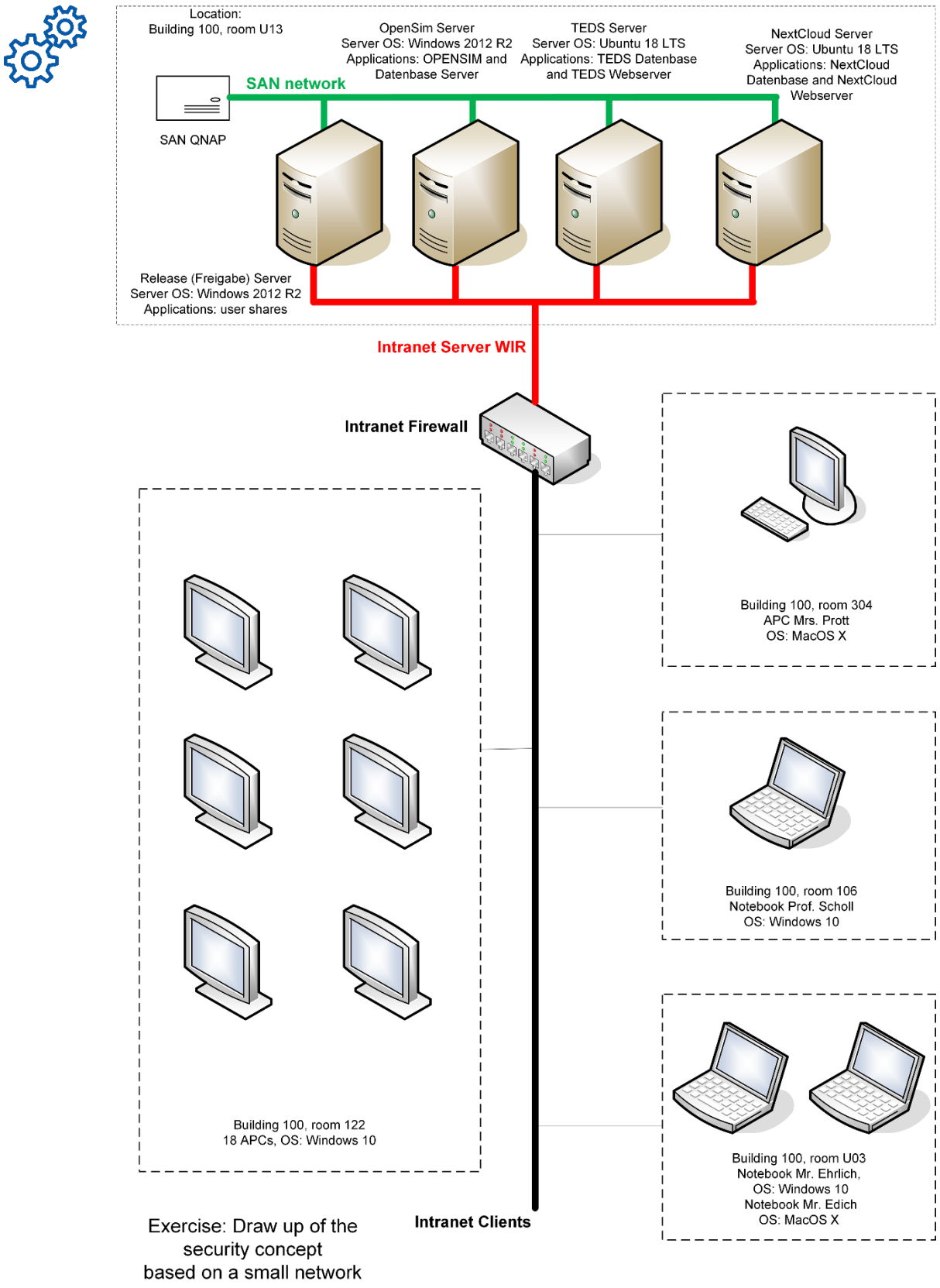


Fig. 15 Example exercise "information domain FS" [Research Group Scholl (in German, "Forschungsgruppe Scholl" or FS)].

For this reason, we show the screenshots of the software used in the German version. However, we think that English-speaking readers who download a free trial version of the software will still be able to understand our example. Our exercise is small and manageable to allow readers to build it independently themselves. We have structured this exercise in a modular way for different target groups. Depending on the course, individual aspects can either be further expanded or reduced. Nonetheless, even our small example illustrates that drawing up a security concept is a complex process.

Software is required for this exercise. The state administrations in both Berlin and Brandenburg have focused on the tool *verinice*, so that we are using this software for our example. Verinice (version 1.20) can be downloaded in a free, open-source version (see [26]) so that readers can follow our proposed exercise as described. The *verinice* tool that is used offers a lot more options, settings, and system properties than we present in this exercise. Our sole aim here is to indicate a practical approach to creating the security concept in line with BSI Standard 200-2 and fig. 16. Our exercise is not intended to be a comprehensive tool-based training but should rather provide useful support in devising the security concept. In a second part, we also give an example of tool-based risk analysis, including consolidation of the security concept and the IT-Grundschutz check (part 2; see fig. 8).

Specify information domain

We will explain the *information domain FS*, an example especially created for this exercise, using the following network plan (fig. 15). This network plan, along with other exercise-relevant documents, is made available for readers in the book's download area. The information domain FS uses various software systems for its external and internal projects. These applications are used by four members of the research group at their office workstations and in the "Laboratory for Administrative Informatics." The students at TH Wildau also have access to some of the applications. A restriction applies that the use of the various software products is only possible via the TH Wildau intranet. Apart from the SAN network, the network infrastructure is completely operated and administered by the university's computer center (in German *Hochschulrechenzentrum* or HRZ) at TH Wildau. The protection needs for the confidentiality, availability, and integrity of the data are classified as *normal*. In the example, we define a *high* protection need for the *confidentiality* of user folders and the intranet of the servers. The network plan (fig. 15) provides a simplified overview of the individual systems and their networking.

Below we show the sequence of steps for the tool-based development of the IS concept for the information domain FS (see figs. 8 and 16):

- Perform a structural analysis and draft the results.
- Carry out a protection requirement assessment.

- Model the information domain.
- Carry out a sample IT-Grundschutz check (part 1) only for the server room
- Plan the implementation of safeguards for the server room.
- Draw up an IT-Grundschutz report for the server room.

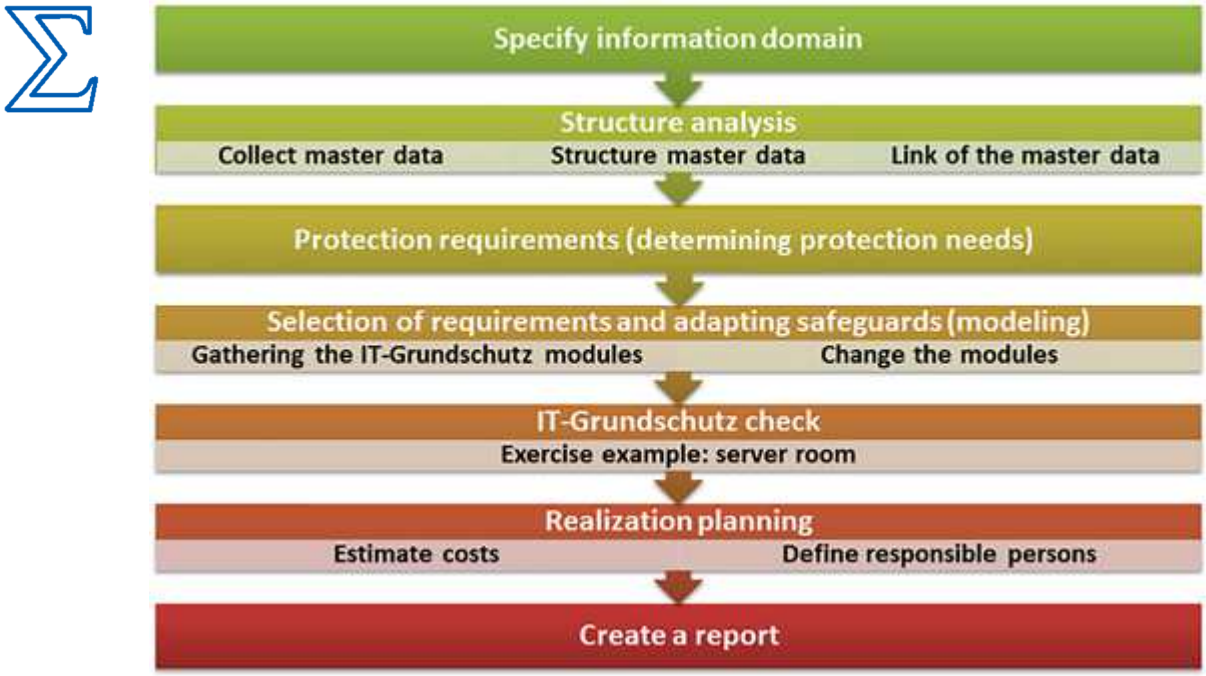


Fig. 16 Model sequence of steps for the tool-based development of an IS concept based on the IT-Grundschutz and standard protection approach (see BSI Standard 200-2 [17]).

3.2 Structural analysis

The structural analysis is a study of the current status of the information domain. It consists of the following three steps: collecting, structuring, and linking the master data.

According to IT-Grundschutz, the goal of the structural analysis is to compile and prepare the necessary knowledge for the information domain. Processes, applications, and IT systems may already have been examined in an initial survey to determine the information domain. Since a graphical network plan of the type presented in fig. 15 provides a helpful additional overview for the tabular compilation of all IT systems, it should be created prior to the analysis. In the structural analysis, these initial documents are completed systematically.

1. Start the *verinice* software and switch to “updated (modernized) BSI basic protection” (*Modernisierter BSI-Grundschutz*) by clicking on the “perspective” option (*Zeige Perspektive*) in the “view” menu (*Ansicht*) (see fig. 17):

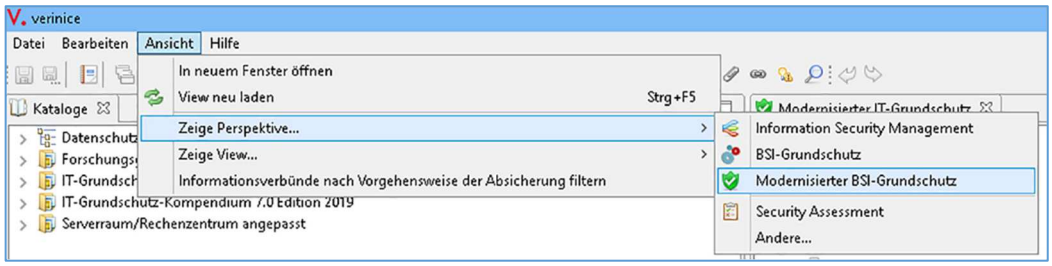


Fig. 17 Changing the perspective view to the updated BSI Grundschutz.

2. For this exercise, you need both the module "IT-Grundschutz Compendium, version 8.0, 2020 edition" and the module "IT-Grundschutz Catalog EL 15 for use in the updated IT-Grundschutz." You can find both downloads on the manufacturer's website at https://verinice.com/produkt/#_download. Import both files using the catalog import function in *verinice* (see fig. 18).

3. Create the information network "Research Group Scholl" (*Forschungsgruppe Scholl*) with the abbreviation FS (see figs. 19 and 20). Select "standard" (*Standard*) for standard protection approach. Then click on the save button in the upper left corner of the screen.

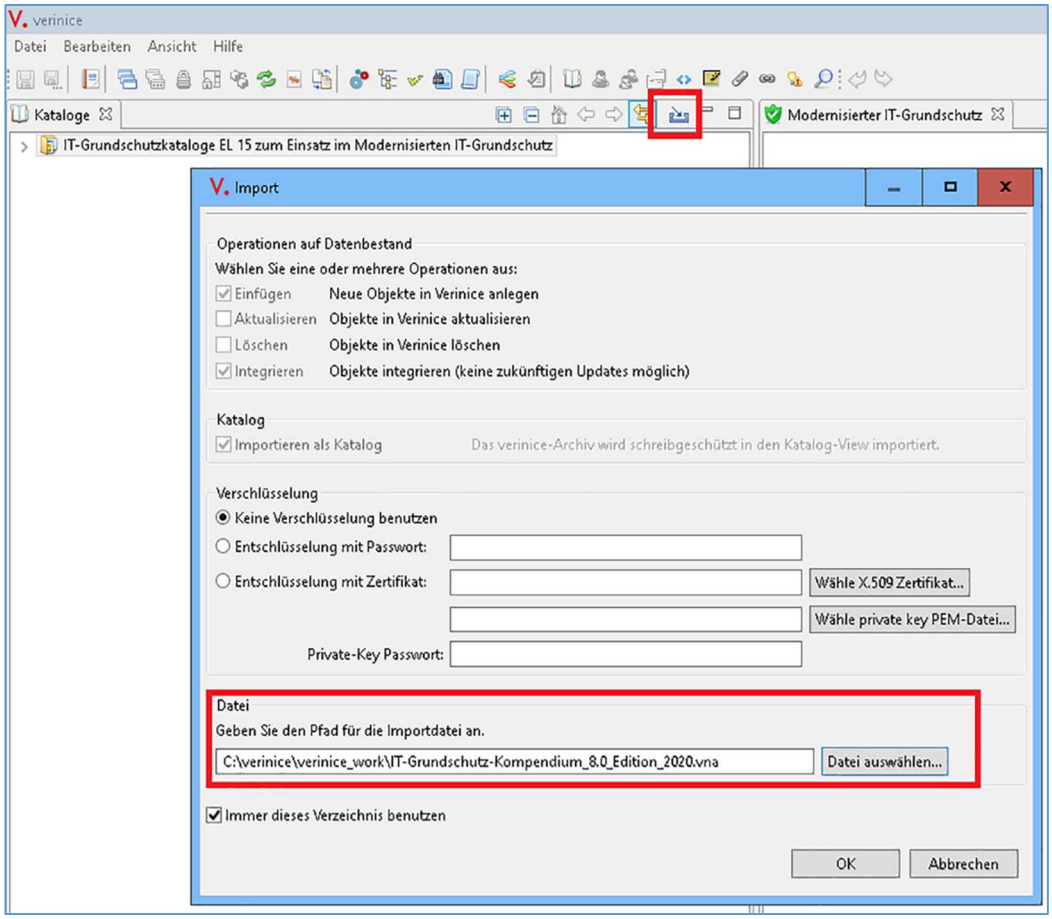


*Fig. 18 Catalog import in the tool verinice. **Note**: The folder c:\verinice\verinice_work is always used as the working folder for all functions such as import, export, and reports.*

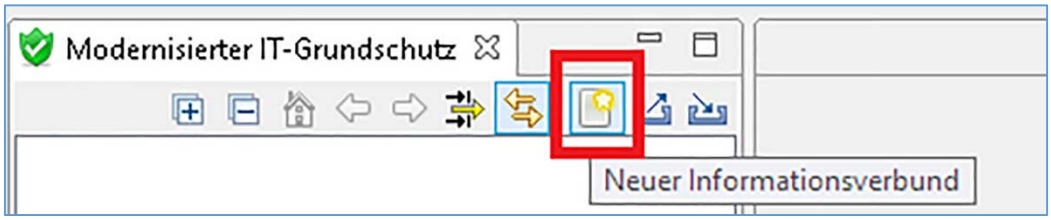


Fig. 19 Creating a new information domain.

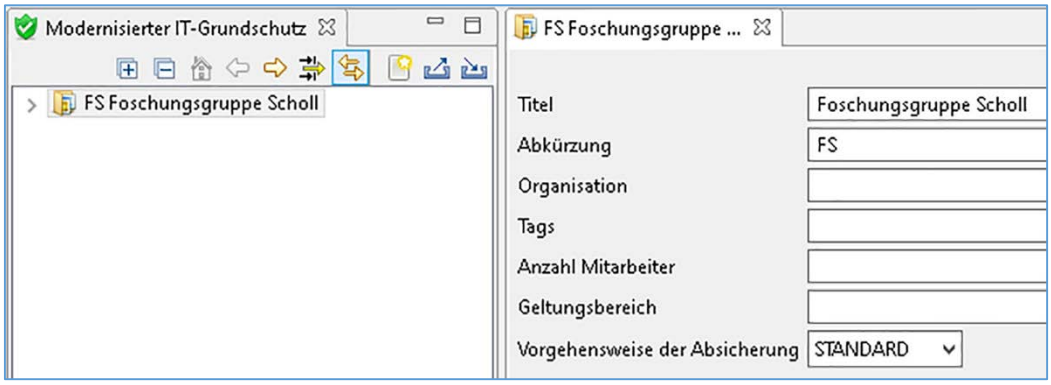


Fig. 20 The Research Group Scholl (Forschungsgruppe Scholl—abbreviated as FS) is created as an information domain.

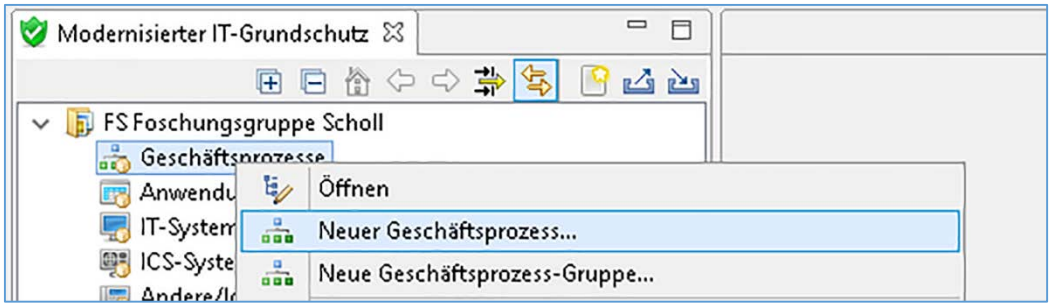


*Fig. 21 Structural analysis in the tool: creating business processes. **Note**: New objects or subgroups below an object group are always created by right-clicking on the respective group.*

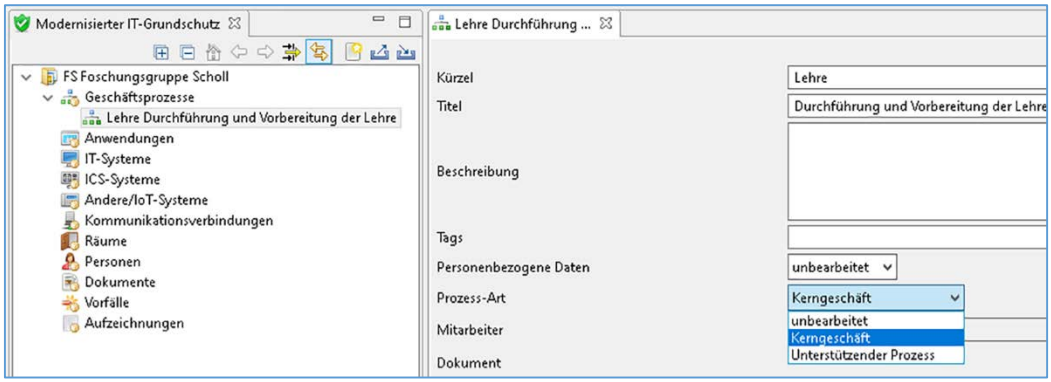


*Fig. 22 The "Lehre" business process is set up as a core business. **Note**: Abbreviations should be unambiguous identifiers that always allow clear assignment within an extensive information domain. Since abbreviations are not absolutely necessary, we will not always work with them in our small sample exercise.*

4. In addition to the various objects from the network plan (fig. 15), we assume that the university's FS research group has only two business processes:
   - "Implementation and preparation of teaching" (*Durchführung und Vorbereitung der Lehre*), abbreviated as "teaching" (*Lehre*)
   - "Administration" (*Administration*)

   Teaching is represented as a "core business" (*Kerngeschäft*) and administration as a "supporting process" (*Unterstützender Prozess)*. Now create these two business processes accordingly (see figs. 21, 22, and 23).

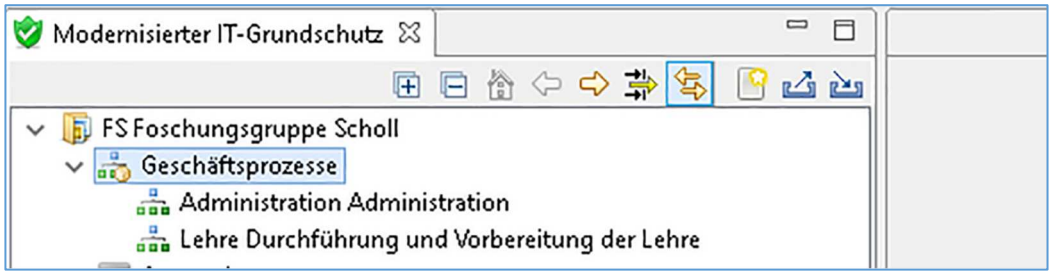


Fig. 23 The two business processes in our sample exercise are created.

After the two business processes in the information domain FS that serve as the starting point for the structural analysis have been created, we use the network plan (fig. 15) to create the IT systems in the tool. Here, for the first time, the so-called *grouping* option can be used. Grouping is an important option for reducing the complexity of objects or the structure of the information domain by creating groups. According to BSI Standard 200-2 [17:66], objects can be assigned to one and the same group "if all components

- are of the same type,
- have similar tasks,
- are subject to similar framework conditions, and
- have the same protection needs."

"In case of technical objects, formation of groups will also be reasonable if they

- are configured similarly,
- are integrated similarly into the network (in the same network segment),
- are subject to similar administrative and infrastructural framework conditions,
- operate similar applications, and
- have the same protection needs.

On the basis of the requirements stated for forming groups, it can be assumed for the purposes of information security that a sample of a group usually represents the security status of the group." [17:66].

5. Study our network plan of the exercise (fig. 15): group (as far as possible) and record all the clients in the information network FS taking into account the grouping rules as follows (see figs. 24–26):

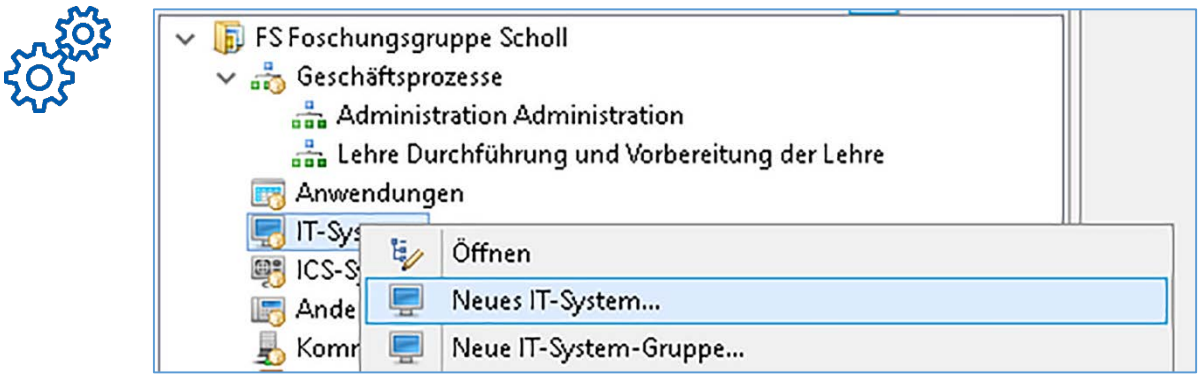


Fig. 24 Structural analysis in the tool: creating an IT system.

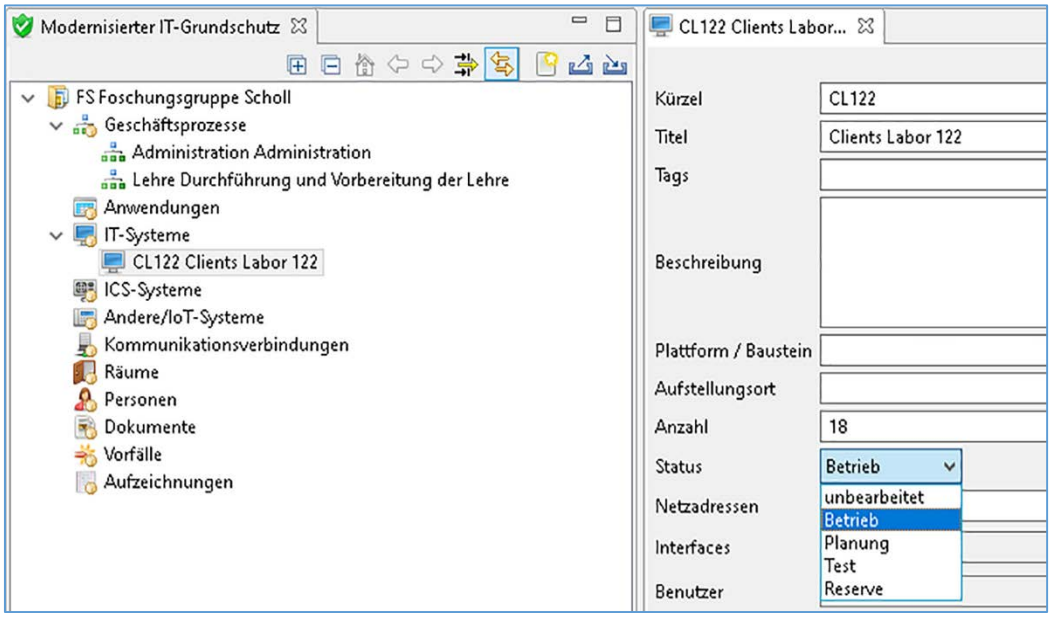


Fig. 25 Creating the clients of the PC Laboratory 122 with the status “Operation” (Betrieb).

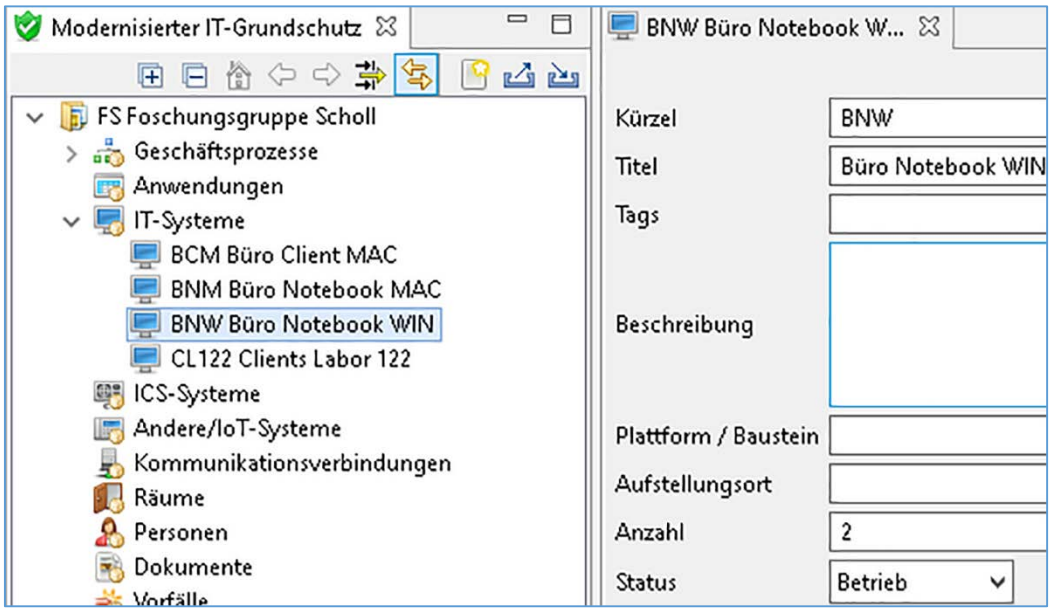


Fig. 26 Four IT system clients of the information domain FS are created in the exercise according to the network plan (fig. 15), taking grouping rules into account.

- 18 clients of the laboratory 122 (CL122)—grouped
- 1 office notebook MAC (BNM)
- 2 office notebooks WIN (BNW)—grouped
- 1 office client MAC (BCM).

We use the expressions in brackets as an abbreviation of the four client systems to be created.

In the next step, we check the servers of the information domain FS (fig. 15) and identify five server systems. With the release server (*Freigabe Server*), for example, files of the FS can be released in the network. With "Nextcloud," the research group FS operates a collaboration platform for online collaboration. The server "OpenSim" stands for Open Simulator and the construction of virtual 3D worlds. The "TEDS" server can be used to carry out evaluations of information artifacts. "SAN" stands for Storage Area Networks and is designed for high-speed transfers of large amounts of data.

6. Create the server systems as an exercise! Since it is not possible to group the servers, all five systems must be created individually (see figs. 27–28):
   - Release server (Freigabe Server, Fserv)
   - NextCloud Server (NextCloudServ)
   - OpenSim Server (OpenSimServ)
   - TEDS server (TEDSServ)
   - QNAP SAN system (QNAP).

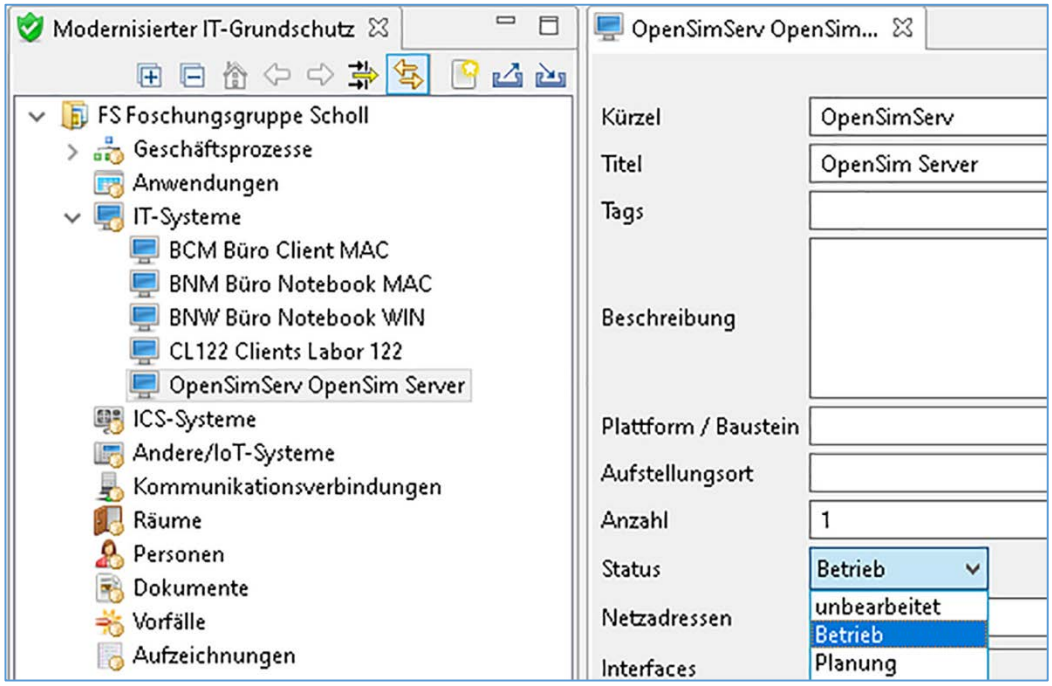


Fig. 27 Creating the "OpenSim" IT server system with the status "Operation" (Betrieb) in the tool.

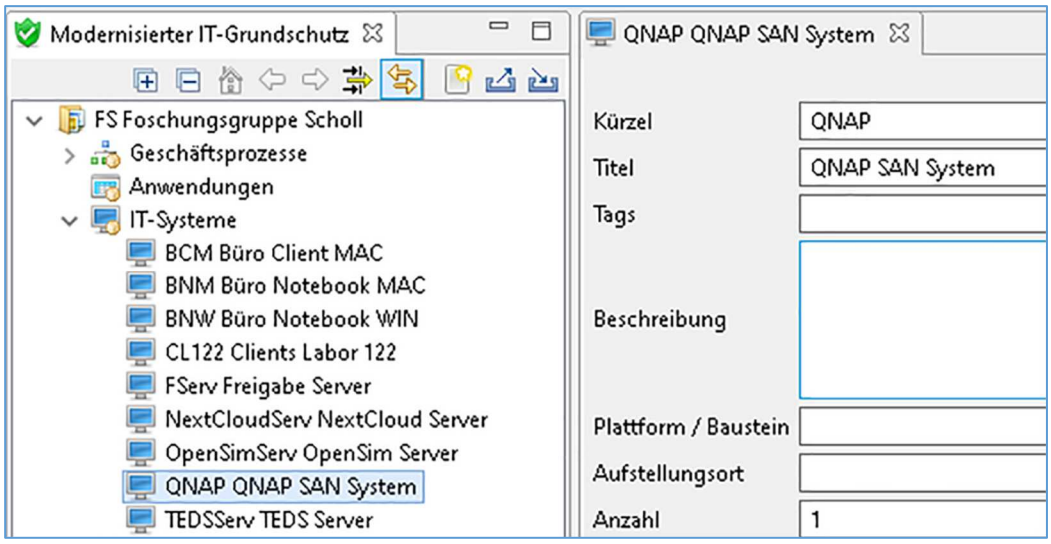


*Fig. 28 All five IT server systems in the information domain FS in the exercise have been created (see the network plan in fig. 15). **Note**: In the case of larger information domains, it makes sense to add further subgroups to the IT system group in order to maintain clarity.*

7. When entering the master data, the communication connections or networks should not be forgotten. Based on this network plan (fig. 15), the three connections visible there are intranet clients, intranet server WIR, and SAN network. They are created in the communication connections of the tool and grouped as follows (fig. 29):

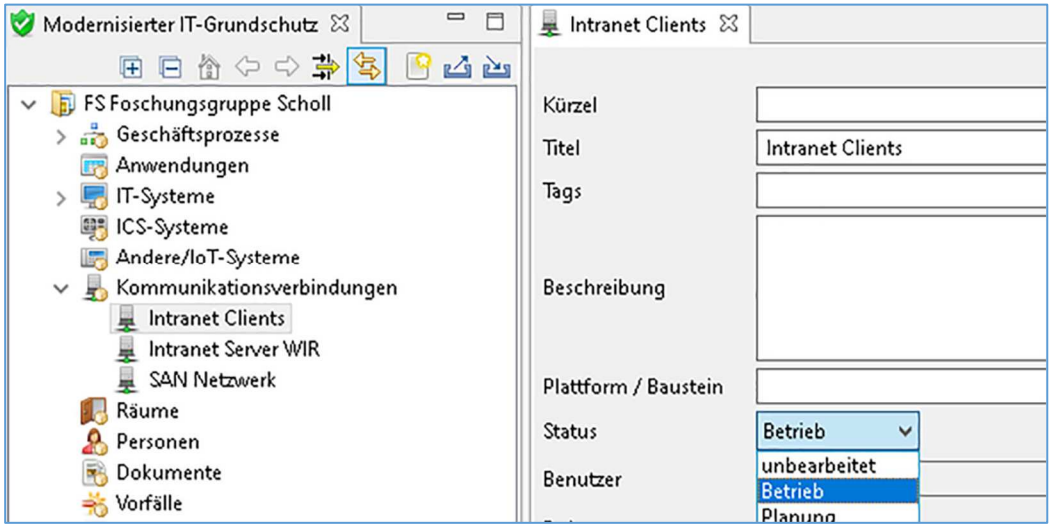


Fig. 29 Structural analysis using the tool: all three networks in the information domain in the exercise are created with the status "Operation" (Betrieb) in accordance with the underlying network plan (fig. 15).

Today, without well-functioning networks, tasks related to digitization will no longer be possible. Therefore, ISOs need to understand the general threats and requirements for networks and their components. For example, the *IT-Grundschutz Compendium* [20] contains the modules *NET: Networks and Communication* with a total of ten modules. We will briefly cover the secure operation of networks, their key components, and a sensible

structure of firewalls in section 5.5 of this book. For the next steps in our exercise, it is important that the networks and communication links in the information domain FS are entered into the tool.

8. After the network acquisition, the intranet firewall is still needed to complete the process of setting up all the active IT systems. In our opinion, it is most useful to assign this to the group “Other/IoT Systems” (*Andere/IoT-Systeme*) (fig. 30):

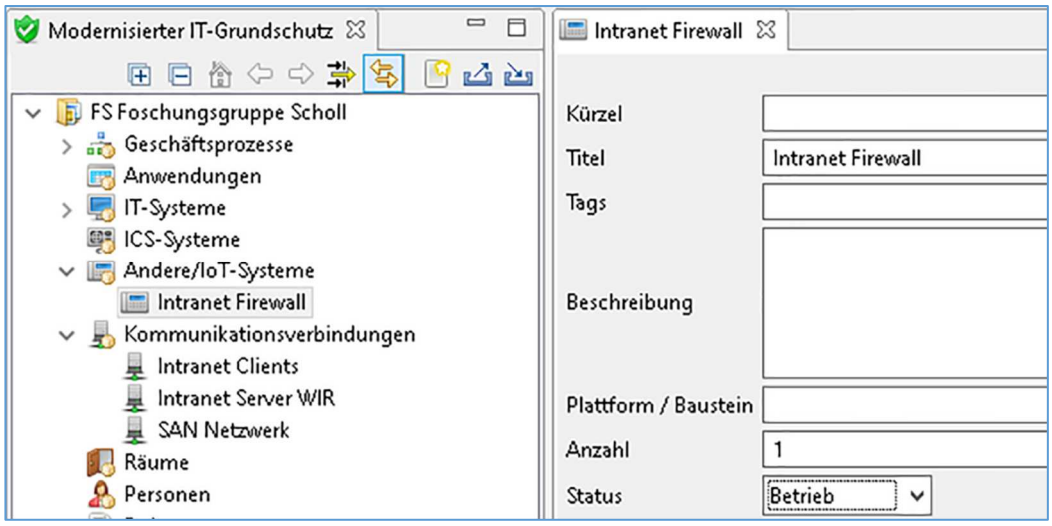


Fig. 30 Structural analysis using the tool: The intranet firewall of the information domain FS in the exercise is set up with the status “Operation” (Betrieb) in accordance with the underlying network plan (fig. 15).

The technical elements of our information network are model components and grouped in the support tool. These are followed in the next steps of the exercise by the software products used, the employees, and the buildings or rooms in accordance with the network plan (fig. 15).

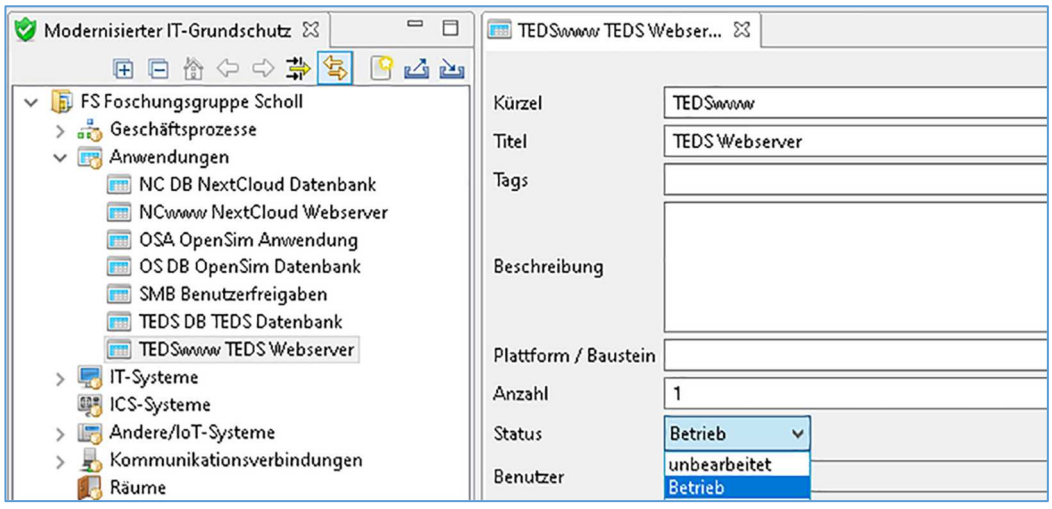


Fig. 31 Structural analysis in the tool: The seven applications of the information domain FS in the exercise are created with the status “Operation” (Betrieb) according to the network plan (fig. 15).

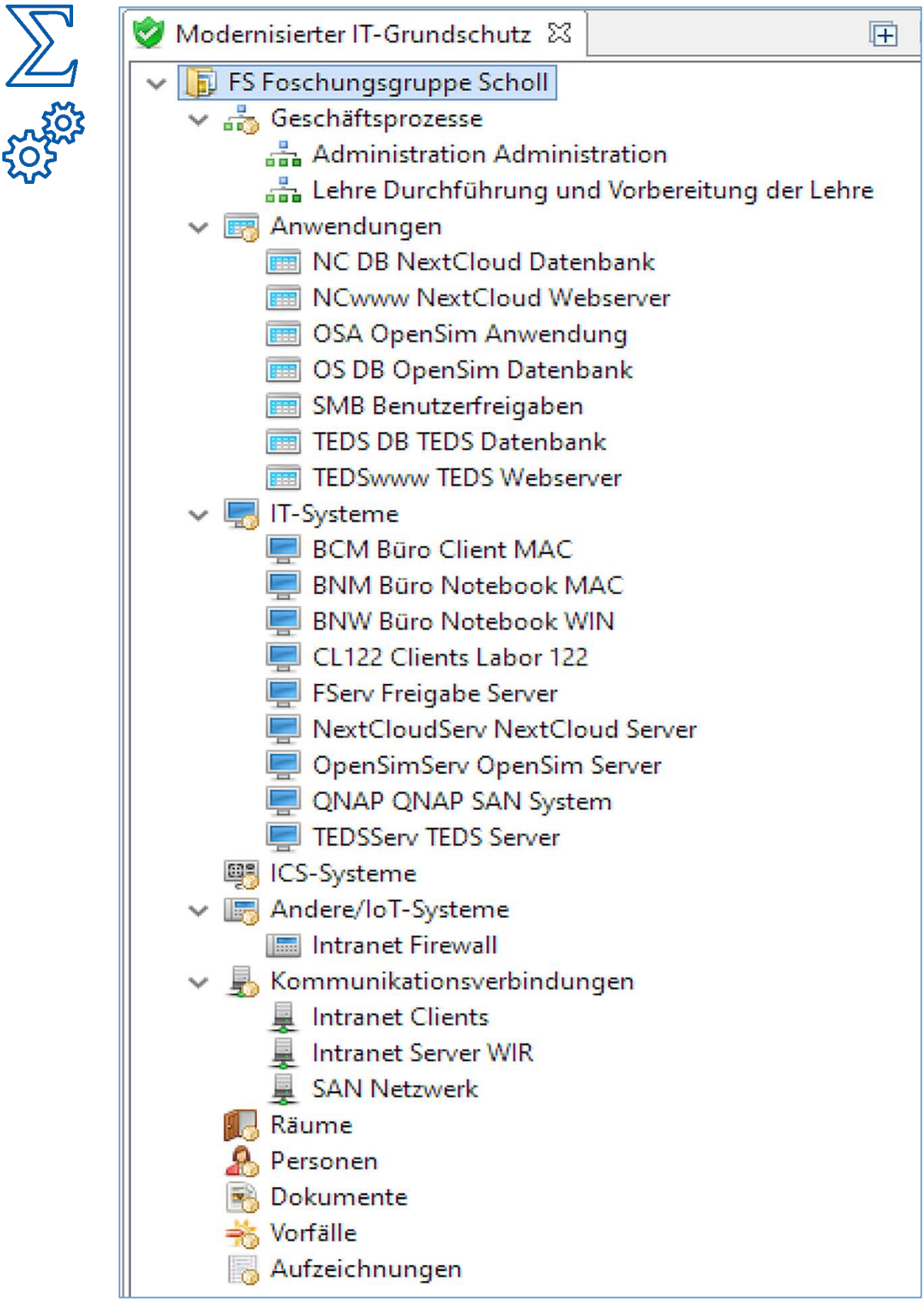


Fig. 32 Interim status I in the structural analysis: master data acquisition modeled for the business processes, the IT systems including networks, and the server software in the information domain FS in the exercise based on the underlying network plan (fig. 15).

9. In the context of this exercise, we limit ourselves to the server applications of the four main server systems in the information domain FS. Based on the network plan in fig. 15, the following seven applications must be recorded in the corresponding group (see figs. 31–32):
   - NextCloud database (NC DB)
   - NextCloud web server (NCwww)
   - OpenSim application (OSA)
   - OpenSim database (OS DB)
   - User approvals (SMB)
   - TEDS database (TEDS DB)
   - TEDS web server (TEDSwww).

The previous intermediate status of master data acquisition modeled in the structural analysis can be seen in fig. 32. We have recorded the business processes, IT systems (clients and servers), and server software as well as networks, components, and communication connections for our defined information network. In order to keep the exercise manageable, we have greatly reduced the complexity inherent in a real-life scenario. If you have followed the exercise yourself using the *verinice* tool, your current status should look like fig. 32.

As personnel for the information domain FS in the exercise, we only include a part of the research group in accordance with the network plan (fig. 15). In addition, there are students from the faculty of the university and the staff of the university computing center (HRZ).

10. The following people should be recorded in the tool as an example (see fig. 33):
    - Students (Stu)—1,000 is the accepted number
    - University computing center (HRZ)—20 is the accepted number
    - Research group—Margit Scholl (MS), Frauke Prott (FP), Denis Edich (DE), and Peter Ehrlich (PE).

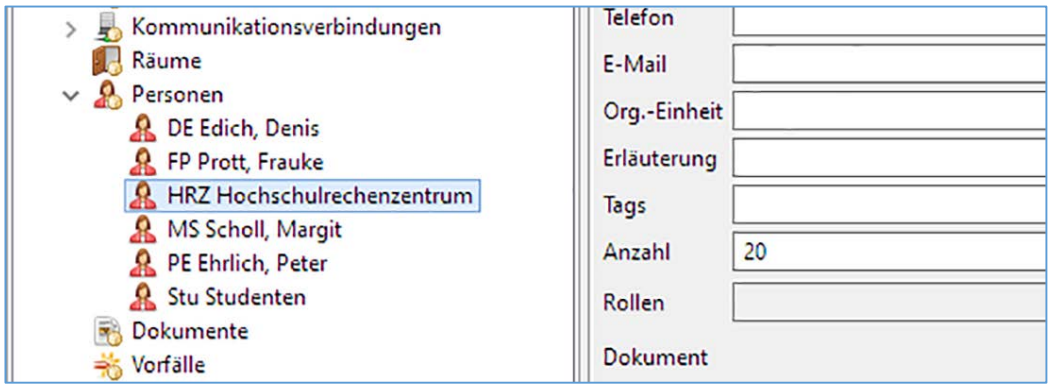


Fig. 33 Structural analysis in the tool: sample recording of various employees and other individuals for the information domain FS in the exercise based on the underlying network plan (fig. 15).

The last step in the master data acquisition within the structural analysis is to create the rooms and buildings. Rooms in IT-Grundschutz and the tool *verinice* are a broad concept that could covering a building or a mobile sales car, for example. We first create the building “Haus 100” on the university campus as a group of rooms and then all the individual rooms within it.

11. As a prelude to registering all the different rooms, it is a good idea to create room groups in advance. Then the individual rooms are created. For our exercise example, right-click on the Research Group FS (*FS Forschungsgruppe Scholl*) to create a room group for building “Haus 100” (see fig. 34):

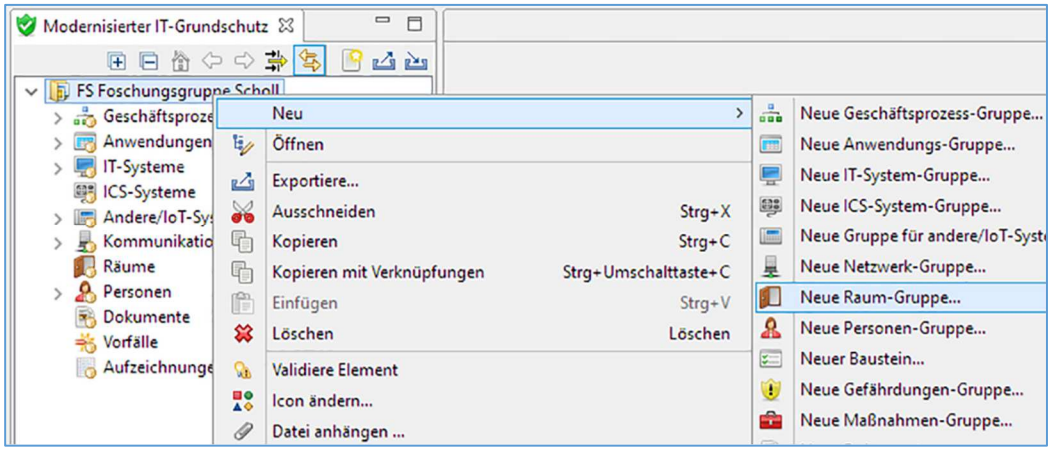


Fig. 34 Structural analysis in the tool: creation of the room group “Buildings” (Gebäude) as part of master data acquisition.

12. For the building in the exercise, “Haus 100” (H100), all the necessary rooms for the information domain FS can be created in accordance with the network plan (fig. 15). The rooms (see fig. 35) are as follows:
    - Laboratory 122 (L122)
    - Room 106 (R106)
    - Room 304 (R304)
    - Room U03 (RU03)
    - Server room U13 (RU13).

Fig. 35 Structural analysis in the tool: All the necessary buildings and rooms for the information domain FS in the exercise are recorded in accordance with the network plan (fig. 15). ***Note****: If you work with several buildings and subunits, it is advantageous to provide the respective rooms with clear abbreviations. In practice, it also makes sense to form different groups of rooms in order to maintain an overview.*

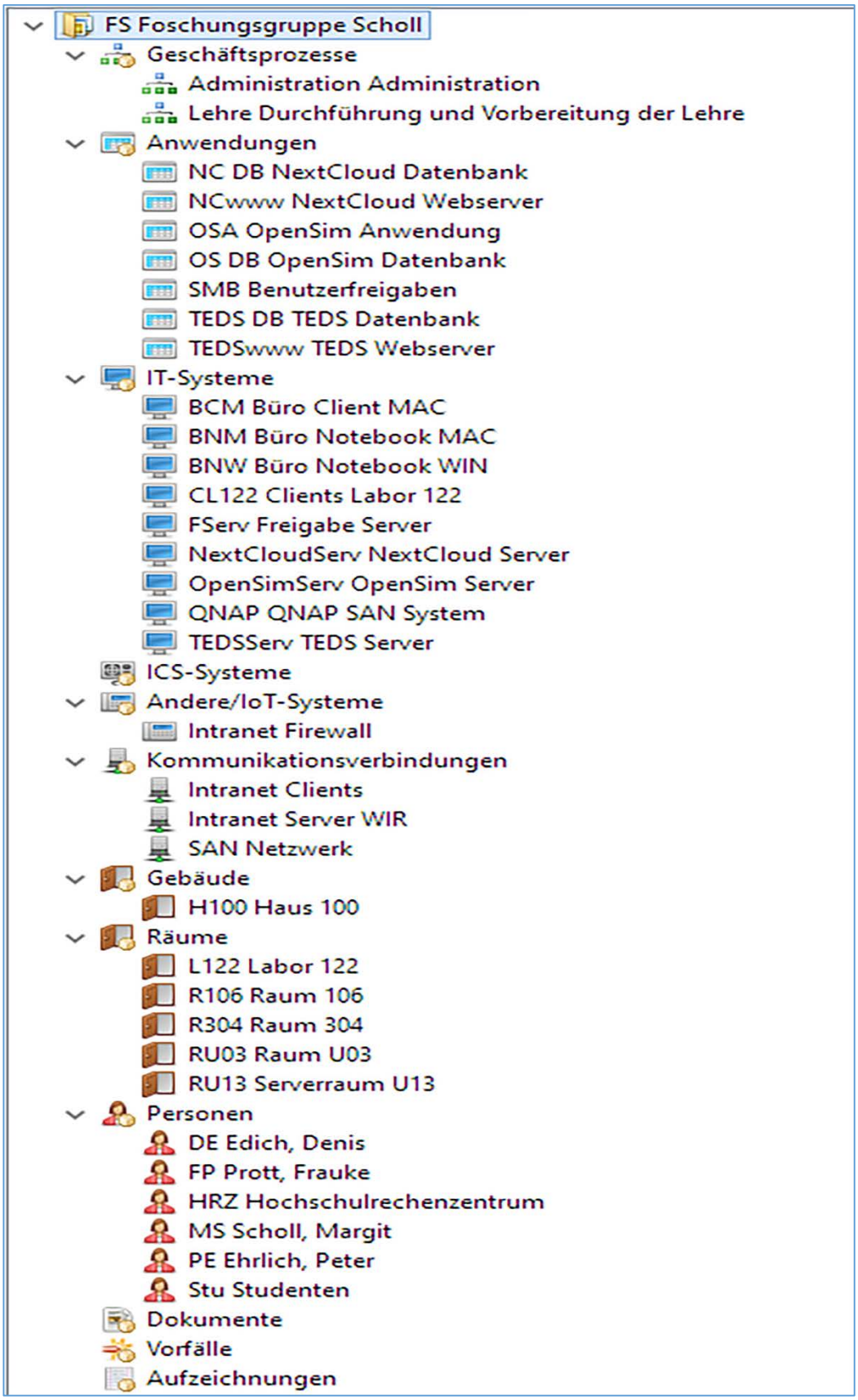


Fig. 36 Intermediate status II in the structural analysis: All the relevant master data for the information domain FS in the exercise is recorded in accordance with the underlying network plan (fig. 15).

The sample master data acquisition is now complete. You can compare your work results using the summary presented in fig. 36. The intermediate status of the master data acquisition for the structural analysis (fig. 36) as a whole forms the inventory of all the objects that have been structured and possibly grouped for the information domain FS. Please note that this is **not** yet a structural analysis but only a categorized inventory. The actual structural analysis now follows. Please refer to fig. 16: it is only in the **third step** that the actual structural analysis takes place, where all the master data needs to be **linked**! According to fig. 16, steps 1 and 2 of the structural analysis have now been completed. This is now followed by the actual work of structural analysis in step 3.

13. The business processes of the information domain FS are linked. To do this, double-click on the administration business process (*Administration*) that you have created, and switch to the links tab (*Verknüpfung*) (fig. 37, bottom right). This enables access to the connection of each structural characteristic that has been recorded.

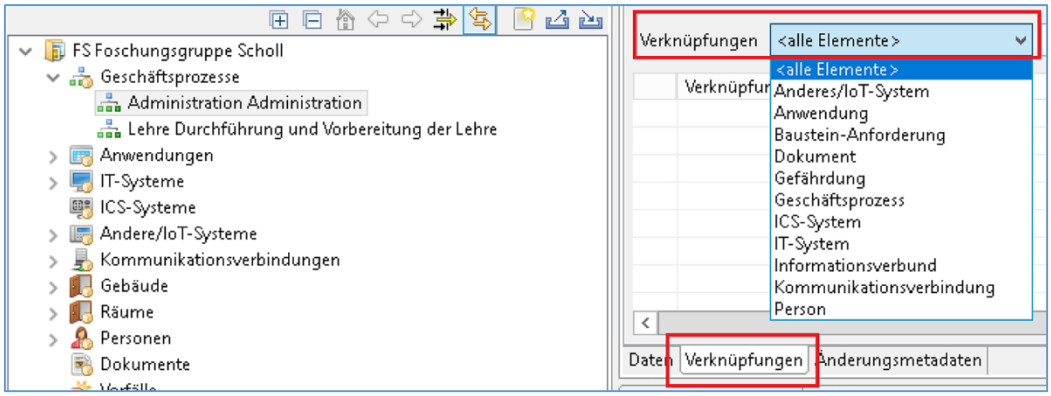


Fig. 37 Step 3: The "linking" aspect of the structural analysis in the tool (see fig. 16). A sample set of linking options based on the master data business process administration (Administration) for the information domain FS in the exercise, based on the network plan used (fig 15).

14. The administration process (*Administration*) supports the teaching process (*Lehre*). At the same time, the names of the responsible persons must be entered in the tool. In order to create the links (*Verknüpfungen*), we first select the desired link targets—e.g., a person in the menu—and click on the "Add" option (*hinzufügen*). Now we can select the relevant people from the full personnel list. Link according to figs. 38-39 and also link the "Teaching" process *(Lehre)* with specific people (see fig. 40).

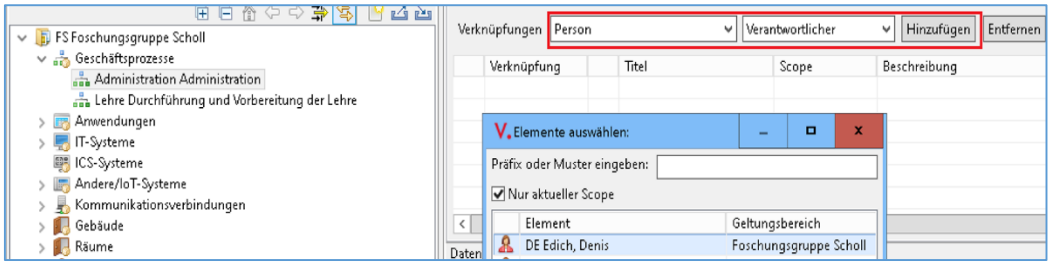


Fig. 38 Step 3, "Linking," in the structural analysis in the tool (see fig. 16): Add three "responsible people" to the process administration (Administration) for the information domain FS in the exercise based on the underlying network plan (fig. 15).

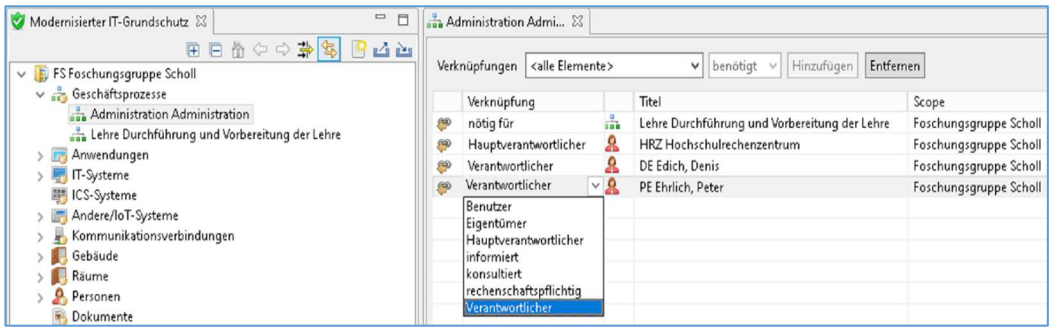


Fig. 39 Step 3 of the structural analysis in the tool: linking the administration process (Administration) with individuals responsible for the information domain FS in the exercise.

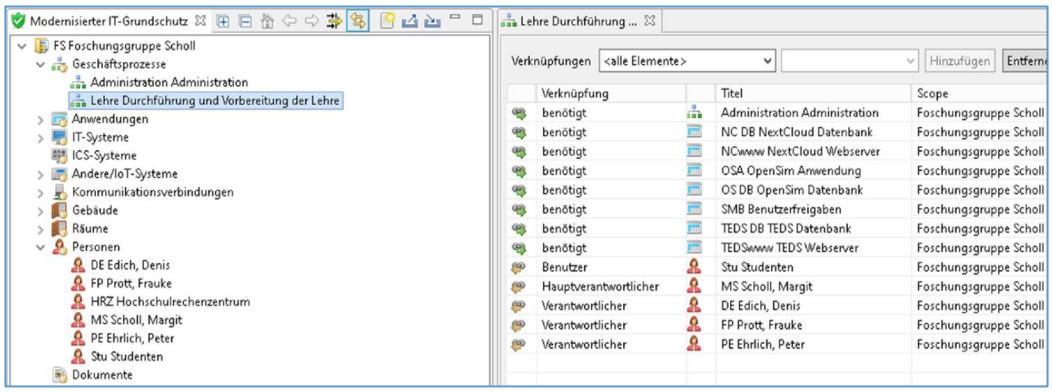


Fig. 40 Step 3 of the structural analysis in the tool: The link between the teaching process (Lehre) and individual people has also been completed for the information domain FS in the exercise.

Initially, a total of seven software products were created for the servers in the exercise. The corresponding links must be created for each of these applications. Readers who understand this structural analysis as part of the tool-based creation of an IT security concept are asked to link all the applications according to their own ideas. Our exercise solution is shown in fig. 41.

15. In the next step, the seven applications entered in the information domain FS are connected to the IT systems and people. To complete the process in real situations, please note that interdependent applications must also be linked to one another. Connect our server applications in the exercise independently using the following illustration (see fig. 41).

16. Analogously, all client IT systems are linked with people, networks, and rooms. Since we have not defined any applications for our client IT systems to simplify this exercise, a direct link to the business processes is necessary (see fig. 42).

17. The server IT systems must also be linked to people, networks, and the server room. Since no application was defined for the QNAP SAN in the exercise, it is linked to the administration process (see fig. 43).

Fig. 41 Step 3 of the structural analysis in the tool: The linking of the individual application is complete. ***Note****: You can mark all the applications by holding down the CTRL key (STRG) and the left mouse button, then release the CTRL key and finally drag and drop the entire group onto the teaching process. The system then closes the manual link screen and creates the link.*

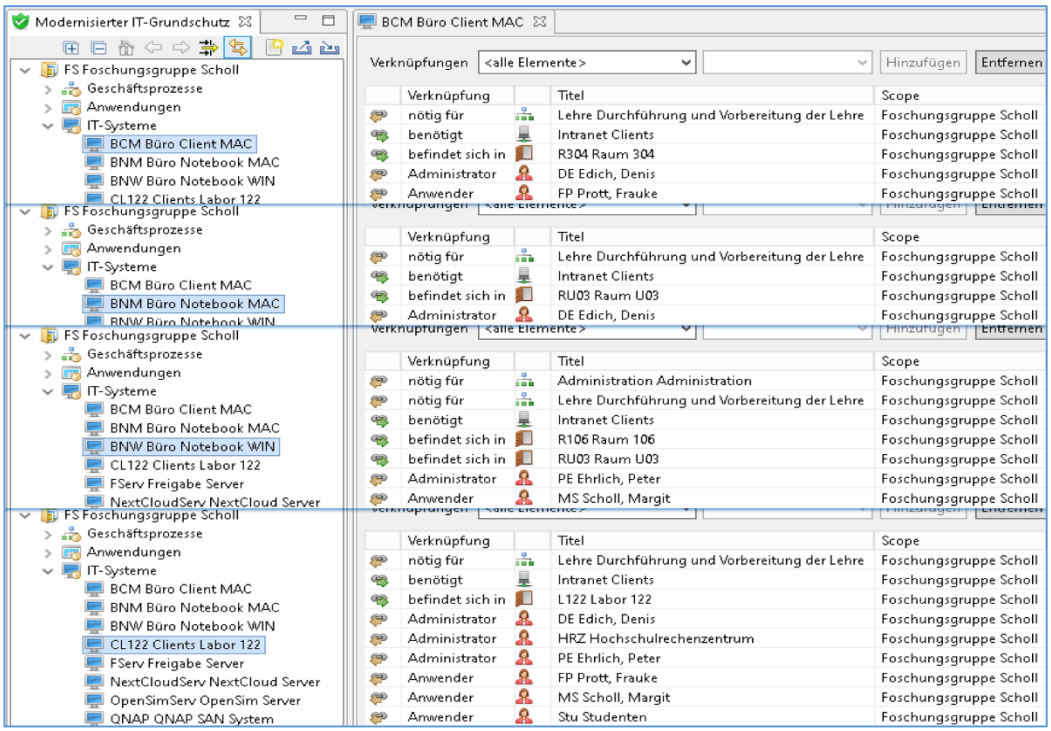


Fig. 42 Step 3 of the structural analysis in the tool: All the client IT systems are linked.

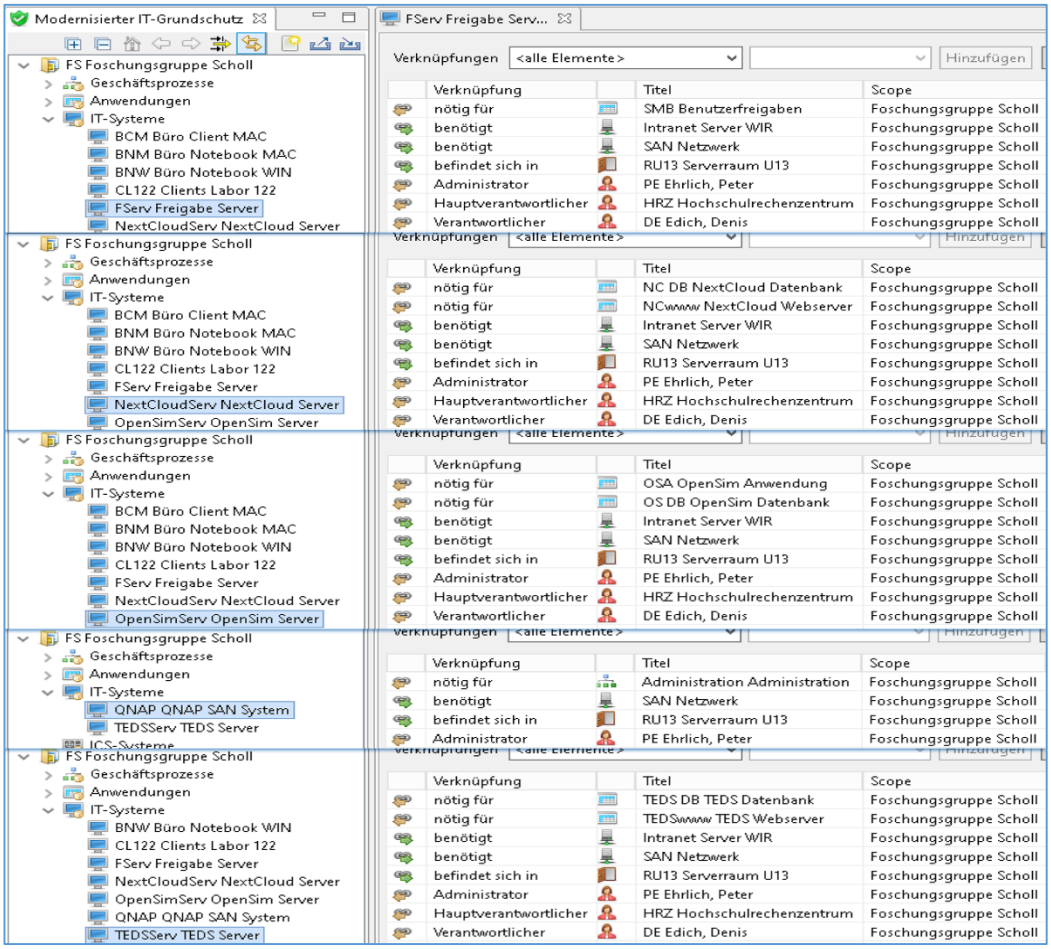


Fig. 43 Step 3 of the structural analysis in the tool: All the server IT systems are linked.

Next, the firewall (reduced to one for the exercise) must be integrated into the structural analysis. There are several ways to illustrate the need for our firewall for business processes. You can treat it as a system without an application and create links to all the other IT systems that communicate with it. Alternatively, you could connect it to the applications or directly to the corresponding business process. For the purposes of our example shown in the network plan, it makes sense to connect the firewall with the IT systems.

18. The next step is to connect the firewall (fig. 44) and the communication connections with the HRZ as the main entity responsible for them. This can be done in the tool using the link view for the HRZ, instead of checking every single communication connection (see fig. 45):

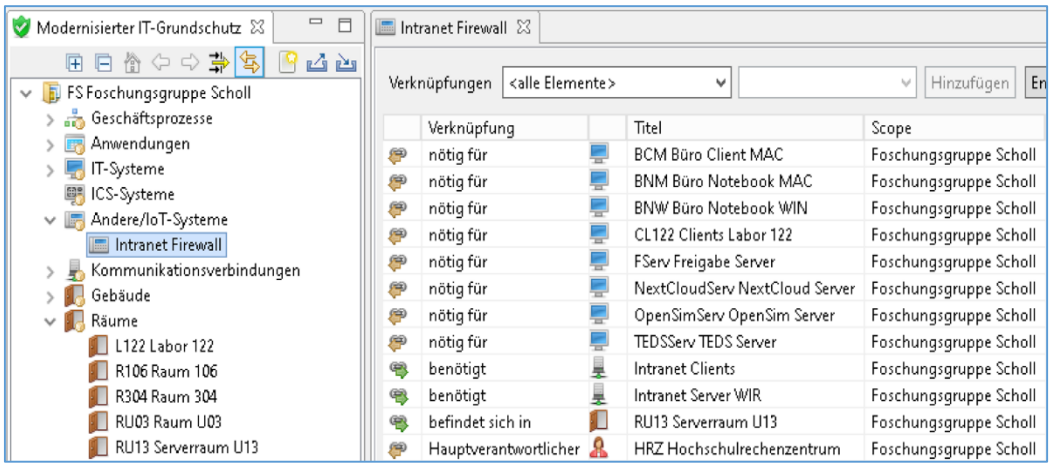


Fig. 44 Step 3 of the structural analysis in the tool: linking the university computing center (HRZ) as the main entity responsible for the intranet firewall. The HRZ is also linked as the main entity responsible for all the networks of the information domain FS.

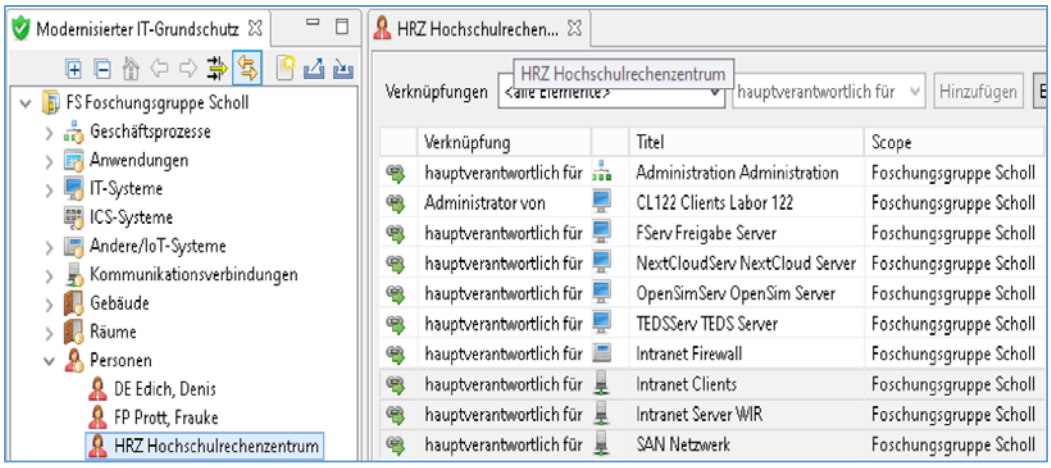


Fig. 45 Step 3 of the structural analysis in the tool: Linking the university computing center (HRZ) as the main entity responsible for all the networks of the information domain FS is completed.

19. The dependency between the building “Haus 100” and the HRZ must also be defined, as shown in the screenshot (fig. 46). In addition, the building must be linked to the rooms, and the people must be assigned (fig. 47).

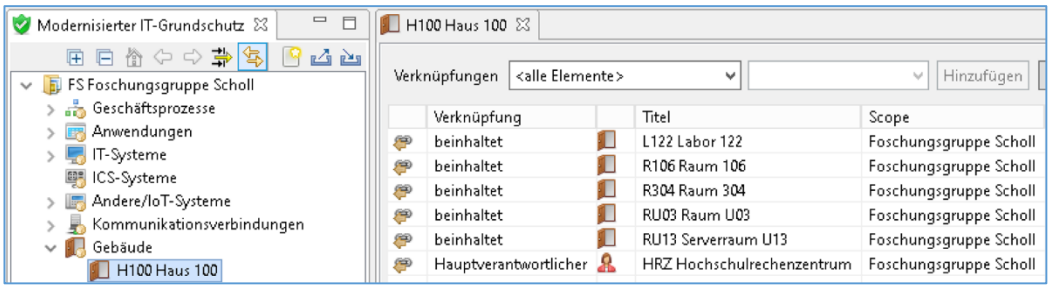


Fig. 46 Step 3 of the structural analysis in the tool: The building "Haus 100" (H100) in the exercise is linked to the HRZ and all the rooms.

The structural analysis in line with the standard protection approach set out in the BSI's IT-Grundschutz is now complete. The master data of *all the objects* in the information domain FS is properly linked.

The structural analysis is not an inventory list. Rather, it assumes the existence of such a list and a current network plan. During the structural analysis, a compilation was made of all the objects that are to be taken into account in the security concept for the defined information domain, but it only becomes an *analysis* when the objects have been properly linked. At this point, you can see how precise the ISO needs to be in involving all the other responsible parties in the security process: management, organizers, specialists, administrators, etc. (fig. 1). The precise nomenclature of the business processes in the information domain also becomes clear. These should be modeled graphically so that interfaces and weaknesses can be seen as quickly as possible. The work of master data acquisition and the modeling of the business processes are absolutely necessary in order to be able to precisely analyze the technical-organizational interaction of all the parties involved and the technical systems.

Space for your personal comments

Personal checklist:

Personal ideas:

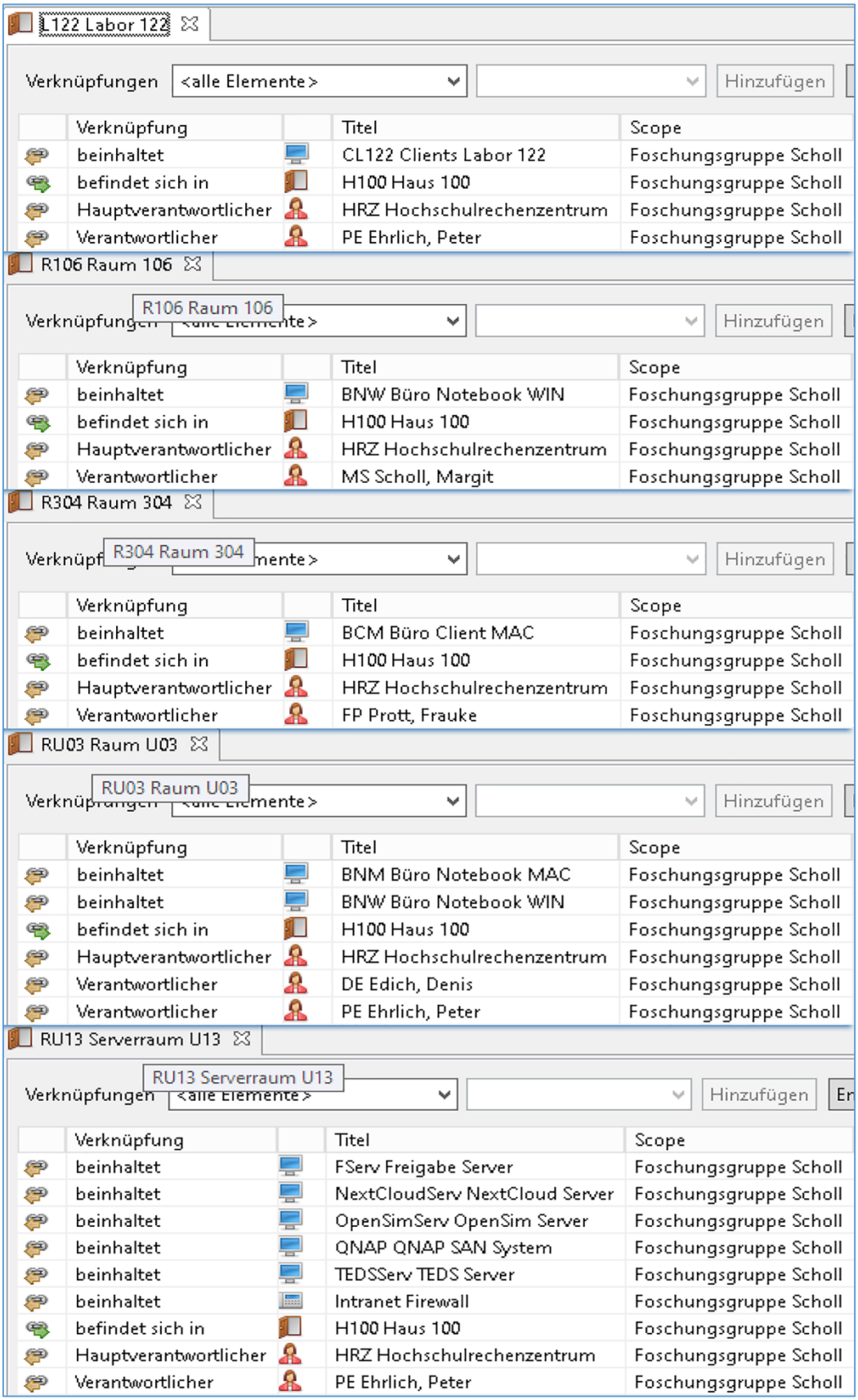


Fig. 47 All the rooms in the building in the exercise scenario (Haus 100, H100) are linked to the responsible persons. The structural analysis of the exercise scenario "Research Group Scholl" (Forschungsgruppe Scholl, FS) is now complete.

3.3 The determination of protection requirements (protection need categories)

After the structural analysis, the protection need categories need to be defined specifically. What do the protection requirements categories “normal,” “high,” and “very high” mean for your entire institution and your specific information domain? For the latter, you have to determine the protection requirements with regard to confidentiality, integrity, and availability for each individual object within the defined information domain. We have already pointed out in chapters 1 and 2 that IT-Grundschutz seeks to ensure a normal level of protection for the standard protection approach. The six damage scenarios from the appendix in BSI Standard 200-2 [17] are helpful in making this assessment. Each institution must clarify its protection needs individually.

The following exercise steps are based, in general, on the assumption of a *normal* protection need (see fig. 16):

1. First of all, the protection need categories for the information society must be defined. After you have double-clicked on the Research Group Scholl (FS), which represents the information domain of this exercise, the *verinice* tool offers the possibility of customizing the categories *non-critical*, *normal*, *high*, and *very high* based on the needs of your organization. Corresponding to the six damage scenarios contained in BSI Standard 200-2 (violation of laws, regulations, or contracts, impairment of the right to informational self-determination, impairment of the physical integrity of a person, impairment of the ability to perform tasks, negative internal or external effects, and financial consequences), you can create individualized definitions in the tool or adopt the BSI defaults (fig. 48):

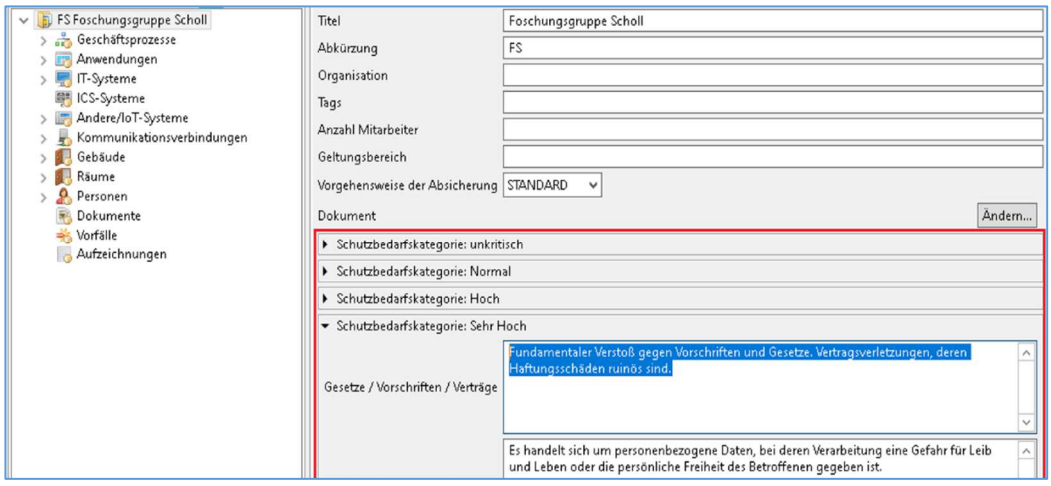


Fig. 48 Example of a definition of the protection need category “very high” in the information domain FS (in German).

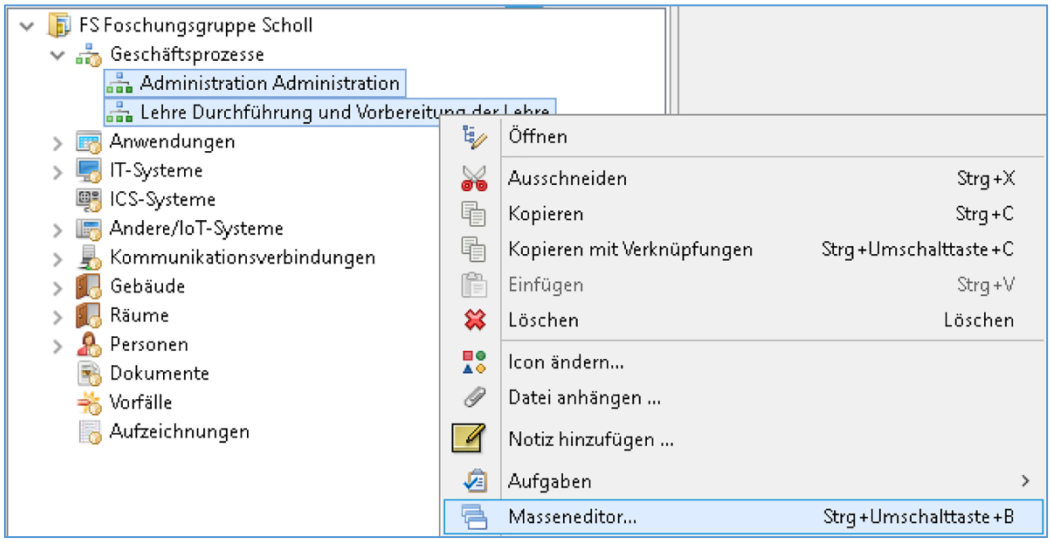


Fig. 49 Using the tool's bulk editor to define the protection need for all the business processes in the information domain FS.

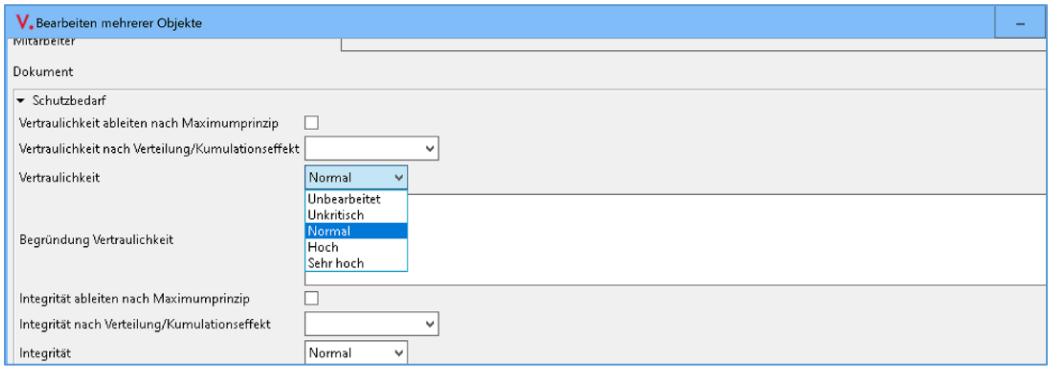


Fig. 50 Assignment of the protection need category "normal" to all business processes.

2. Since neither of the two business processes in the information domain FS created in the exercise has an increased need for protection, we define these as normal. Using the tool's bulk editor, you can do this in one step by making the selection and right-clicking (figs. 49 and 50):

3. The next step is to check all the applications. In our scenario, we assume that only the protection needs of the user clearances are classified as "high" in the area of confidentiality, since personal data is processed. This must be set explicitly in the tool (see fig. 51). Using this assumption, we can show a risk analysis in our exercise later on.

Note that the tool automatically specifies the *maximum principle* for all three basic IS values—this may need to be changed (see fig. 51, right). For our exercise, we therefore remove the maximum principle for the basic value of confidentiality for the user clearances ("SMB Benutzerfreigaben") application in order to be able to determine a *high* protection need with regard to the personal data that has been processed. However, we leave the maximum principle for all the other applications.

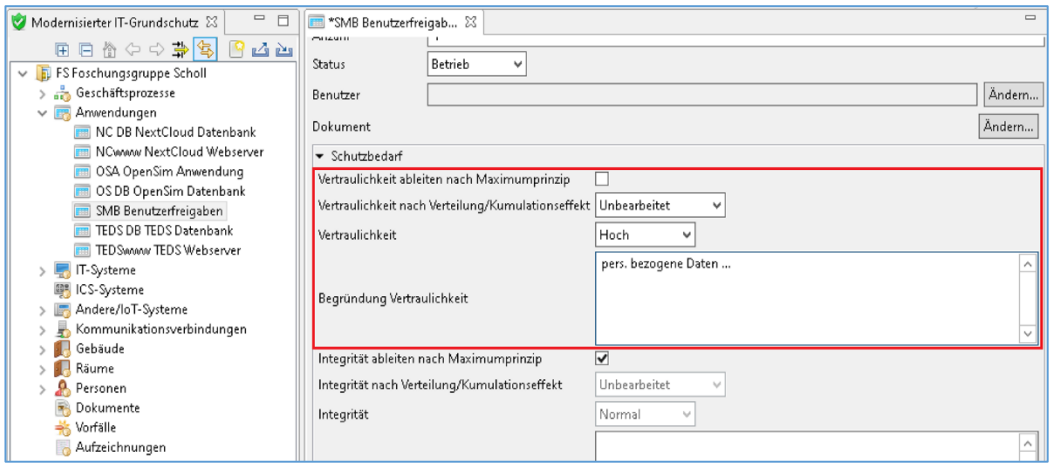


Fig. 51 Determining the protection needs for the user clearance application "SMB Benutzerfreigaben." For practice purposes, the maximum principle for the basic value of confidentiality should be removed so that a high protection need can be set.

The abolition of the maximum principle in fig. 51 has further consequences for the linked clearance server "FServ Freigabe Server" (see fig. 52).

4. The protection need for the linked clearance server "FServ Freigabe Server" must be checked according to fig. 52. We retain the maximum principle for all the other IT systems.

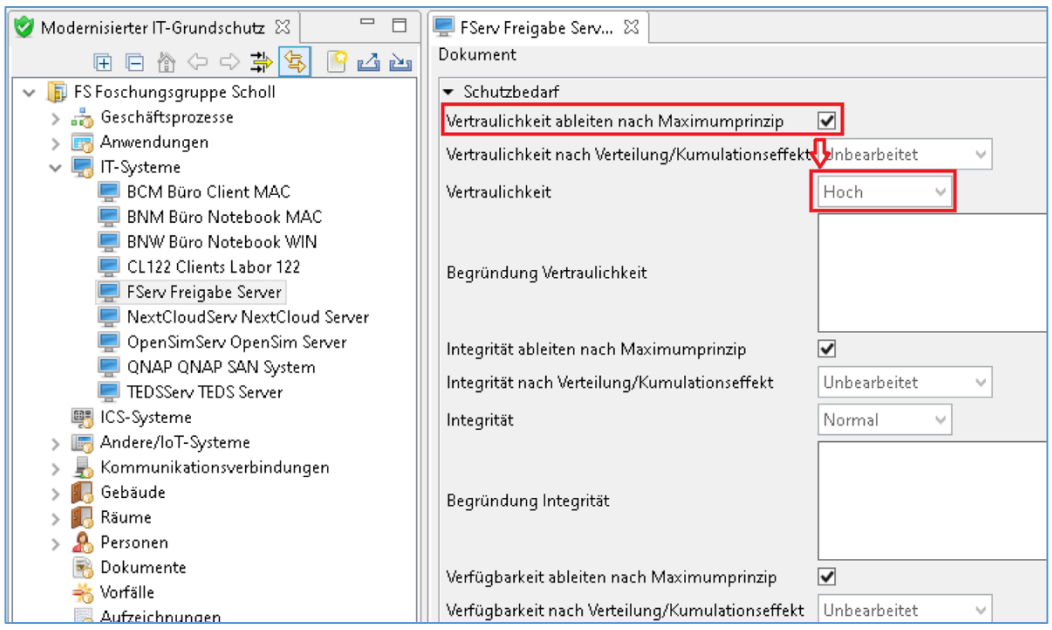


Fig. 52 Checking the protection requirement determination for the linked clearance server "FServ Freigabe Server." The maximum principle triggers a high protection requirement for the basic value of confidentiality.

Next, the need to protect the networks is checked in this exercise. Note how, according to the maximum principle, the high level of protection from one application was inherited by the structures via the individual links in the structural analysis.

For exercise purposes, we define two exceptions to the maximum principle for the following reasons:

- Because the SAN network, as an encapsulated network, contains only encrypted, temporary backups, a normal protection requirement with regard to confidentiality is sufficient. Since only temporary backups are included, no impact on overall operations is expected in the event of a malfunction. Therefore, its availability can even be downgraded to “non-critical” based on the “distributive effect” (see fig. 53).
- Because of the maximum principle, the “WIR intranet server” already has a high need for protection with regard to confidentiality. Since none of the server processes are available without this particular network, a “high” protection need with regard to its availability is also required based on the “cumulative effect” (fig. 54).

5. All the settings for the networks that have been created and linked need to be checked—we leave the maximum principle in place in all instances except for the SAN network. For exercise purposes, we specify a “normal” protection need for the SAN network (fig. 53):

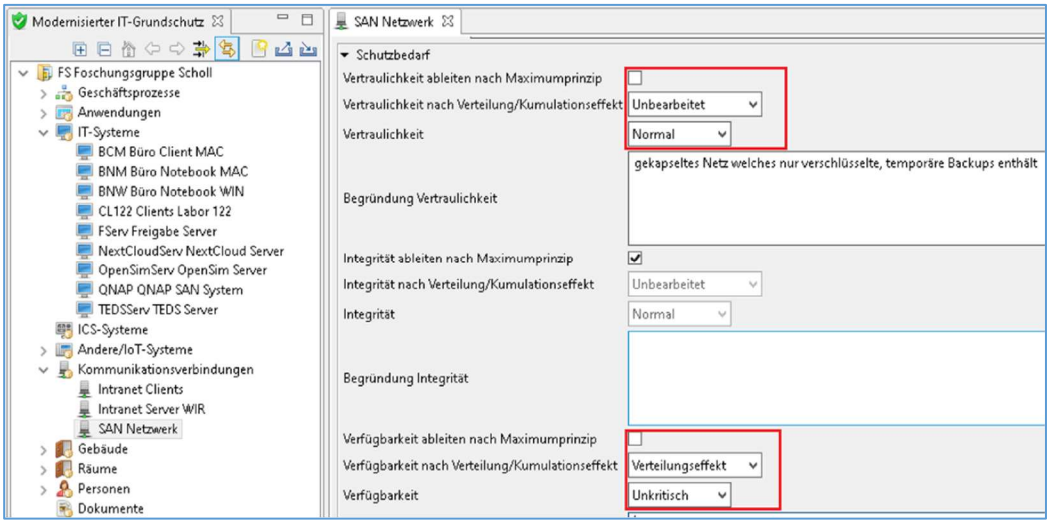


Fig. 53 Determination of protection needs for the “SAN network” (see fig. 15). Because we are dealing here with encrypted, temporary backups of the server, the high protection requirement that was inherited is reset to “normal” in the exercise.

6. The protection need categories for the “WIR” intranet server are determined according to fig. 54. Set the values accordingly in your own tool. The client network is separated from the server network by the firewall and therefore only a normal protection requirement for all three basic values is set.

7. The protection needs and the links of the intranet firewall must be checked (fig. 55). No changes are required in the protection requirements check for the intranet firewall, since the maximum principle has correctly defined the protection needs via the linked clearance server.

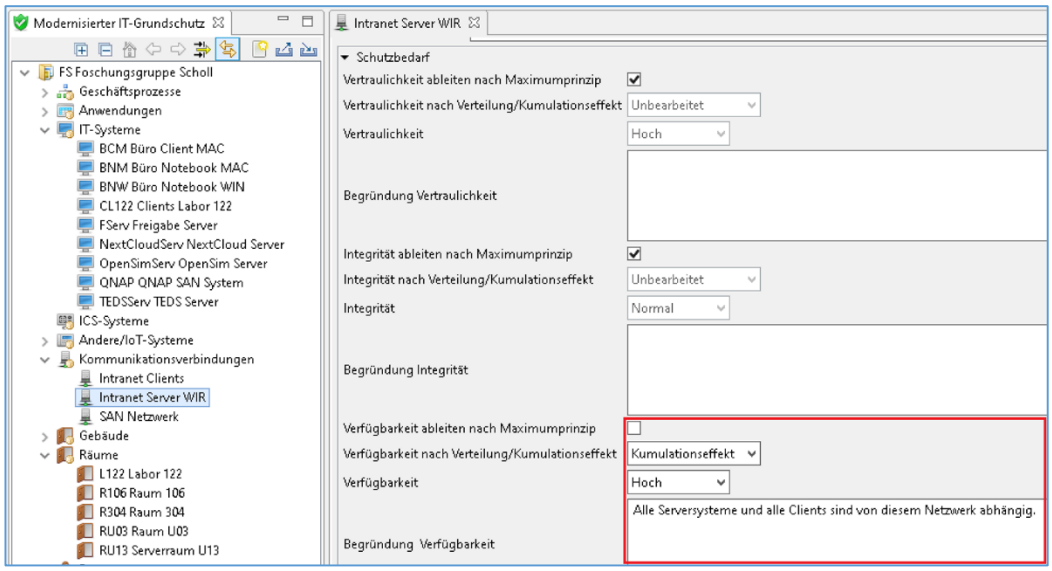


Fig. 54 Protection need determination for the intranet server "WIR".

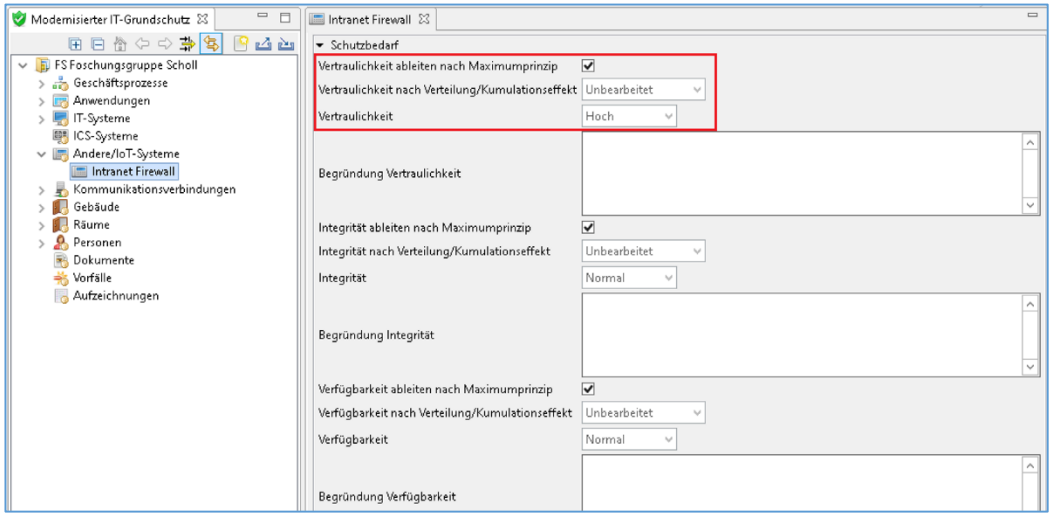


Fig. 55 Protection need determination for the intranet firewall. In our exercise, no changes are required in the protection requirements check for the intranet firewall.

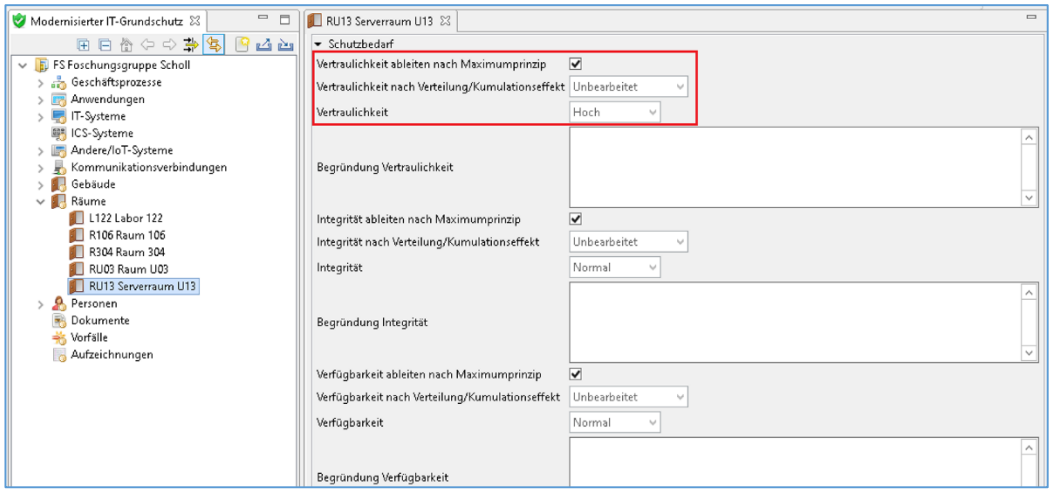


Fig. 56 Checking the protection need settings for the server room of the information domain in the exercise.

After setting the protection requirements for all the IT systems, the on-site rooms can be checked to monitor their protection needs. As expected, according to the maximum principle, a high protection requirement applies only to the server room (fig. 56).

8. The protection requirements of the server room must be checked according to fig. 56.

As the last step in this tool-based exercise, the building “Haus 100” should be checked, because its protection requirements must also be derived from the previous protection settings. The inheritance rules must be checked in the tool. The protection requirement is set to normal for this publicly accessible university building. For this purpose, the maximum principle as an inheritance principle for the basic value of confidentiality is lifted and the distributive effect is set in the tool (see fig. 57). However, the server room security must be adequately designed with a high protection need in the subsequent model.

9. The protection requirements for the building “Haus 100” are adjusted in accordance with fig. 57.

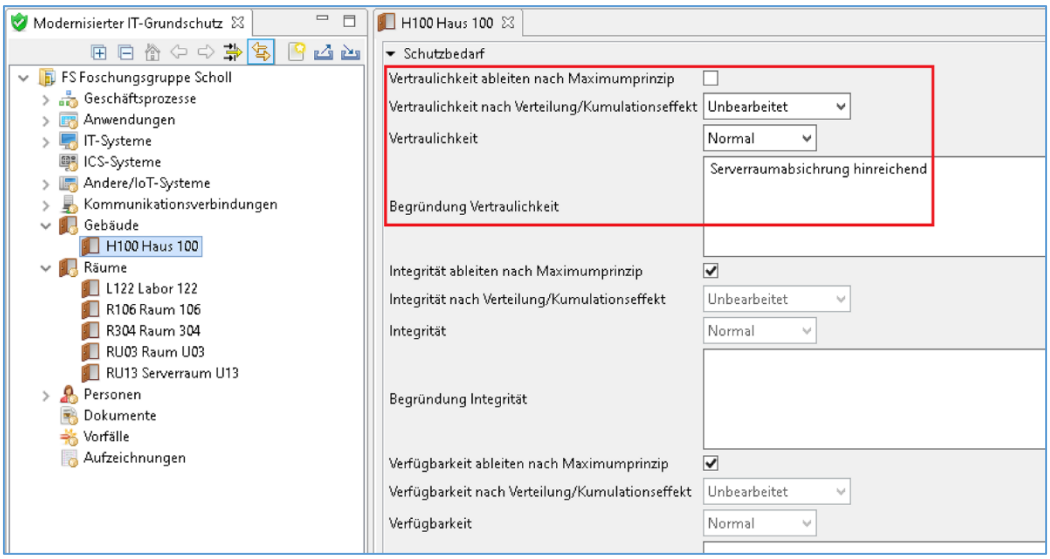


Fig. 57 Checking the protection needs determined for the university building in the information domain in the exercise. A normal protection requirement should apply to all three basic values. In the exercise, we remove the inheritance of the maximum principle (a high level of protection from the server room to the entire building) and define a normal level of protection for the building, even for the basic value of confidentiality.

Our exercise on the tool-based determination of protection needs has been completed, and we can now turn to modeling (see fig. 16). It should be noted that, according to IT-Grundschutz, a normal protection requirement means that it is generally sufficient to meet the standard security requirements. If the protection requirement of a target object is determined to be *high* or *very high*, a *risk analysis* is necessary.

3.4 Modeling

In the IT-Grundschutz approach, *modeling* means the selection of security requirements. In principle, this consists of two steps (see fig. 16): first, the acquisition of the modules of the *IT-Grundschutz Compendium* and second, if necessary, the modification of these modules. The latter might be the case, for example, if there is no immediately suitable module—and therefore a similar module is used—or a separate module is defined as a result of a risk analysis. Each suitable module describes the requirements that have to be met with measures for a desired level of protection. In the following exercise, we will limit ourselves to just a few examples to achieve a normal protection requirement and then focus on the server room in the risk analysis. The high protection need is only taken into account for the subsequent risk analysis.

The aim of the modeling as per IT-Grundschutz is to assign appropriate modules from the *IT-Grundschutz Compendium* for each systematically linked object in the selected information domain based on the protection need that has been defined and justified, and to decide which of the identified security requirements must or should be fulfilled, and which measures from the implementation guidelines would be suitable for this.

We model our FS information network as an example, including some overall features of the following process components from the *IT-Grundschutz Compendium* [20]:

- ISMS.1 Information security management systems
- ORP.1 Organization
- ORP.2 Staff
- CON.1 Crypto concept
- CON.2 Data protection
- CON.7 Information security when traveling abroad
- OPS.2.1 Outsourcing for customers
- OPS.3.1 Outsourcing for service providers
- DER.2.1 Handling security incidents
- DER.4 Business continuity management.

The modeling in the *verinice* tool consists of an automatic link, which is applied to the relevant modules using drag and drop. Therefore, at the beginning of the modeling of an information domain, the necessary modules must be selected from the *IT-Grundschutz Compendium* for the entire information domain.

This list only represents a small selection of all the necessary modules. When setting up the exercise, we used the current *IT-Grundschutz Compendium*, version 8.0, 2020 edition.

1. Mark all of the modules in the list and drag them to the Research Group Scholl “FS Forschungsgruppe Scholl” for modeling (see fig. 58, left side):

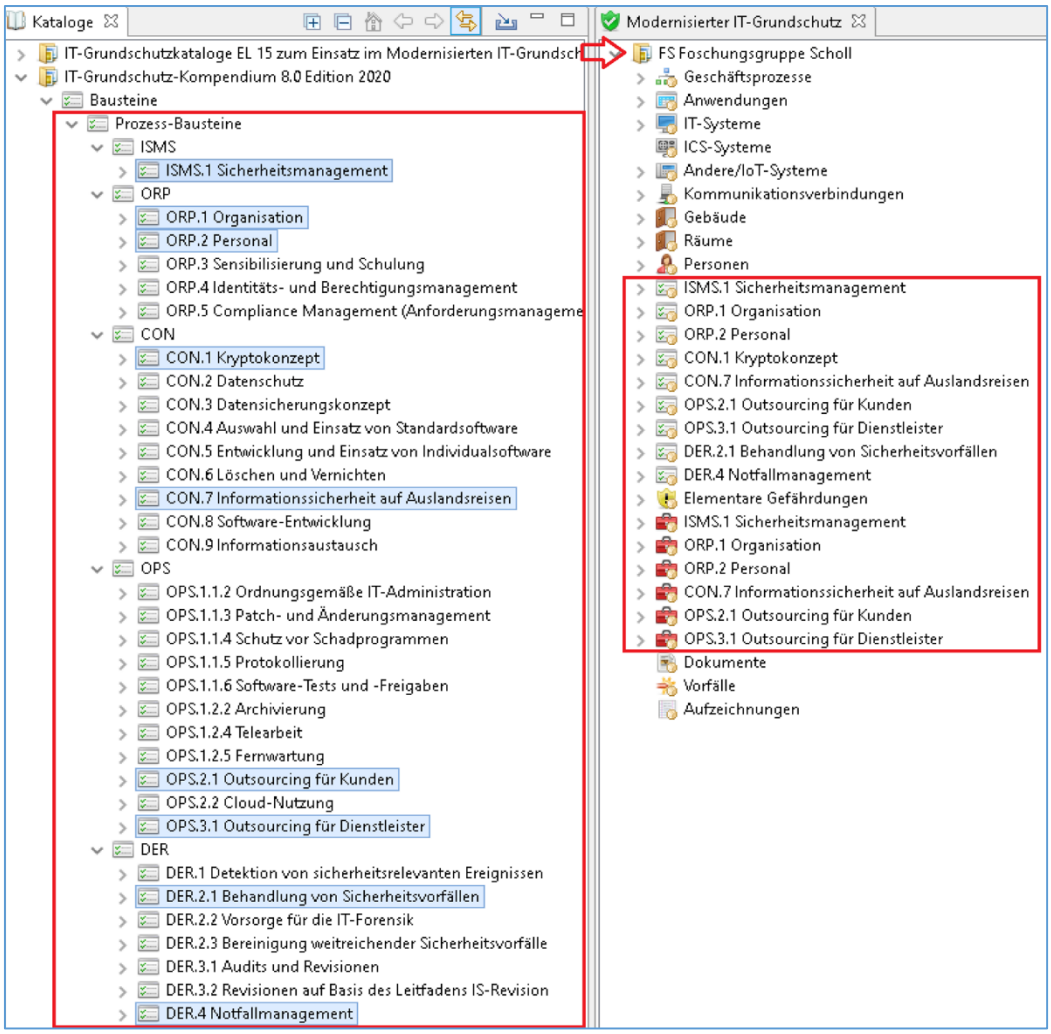


Fig. 58 The IT Grundschutz Compendium, version 8.0, 2020 edition, used for this exercise in the verinice *tool (left): modeling of some modules from the list directly on the information domain (drag marked modules to the right). The result is seen in the red box on the right.*

If, for example, the module ISMS.1 is clicked on, all the modeled parts of the security management module in the FS information domain as well as the ISMS.1.A1 requirement are shown as examples. In addition to the module requirements, the threats that can be reduced as well as the necessary measures were linked in the form of instructions (see fig. 59).

In the case of a larger information domain, you can organize the modules, the threats, and the measures in your own subfolders after the modeling. This is done in the same way as for the building of a room group (see fig. 34).

2. Take a look at the basic requirement ISMS.1.A1 in the domain you have created—as per fig. 59:

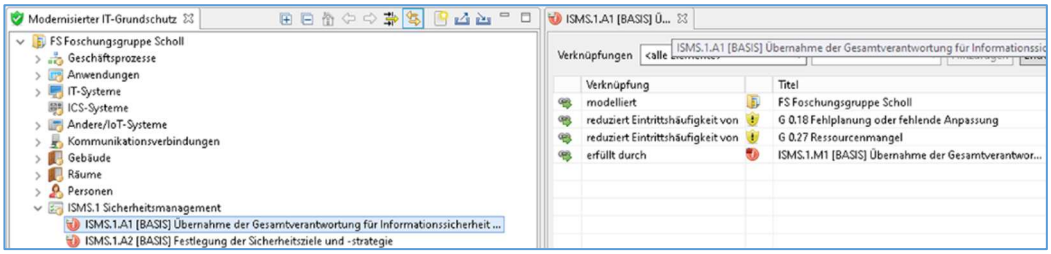


Fig. 59 Modeling details for ISMS.1.A1 for the information domain FS.

3. Now model the CON.3 module directly for the administration process. Here too, the modules, threats, and measures are created in groups and are automatically linked (fig. 60):

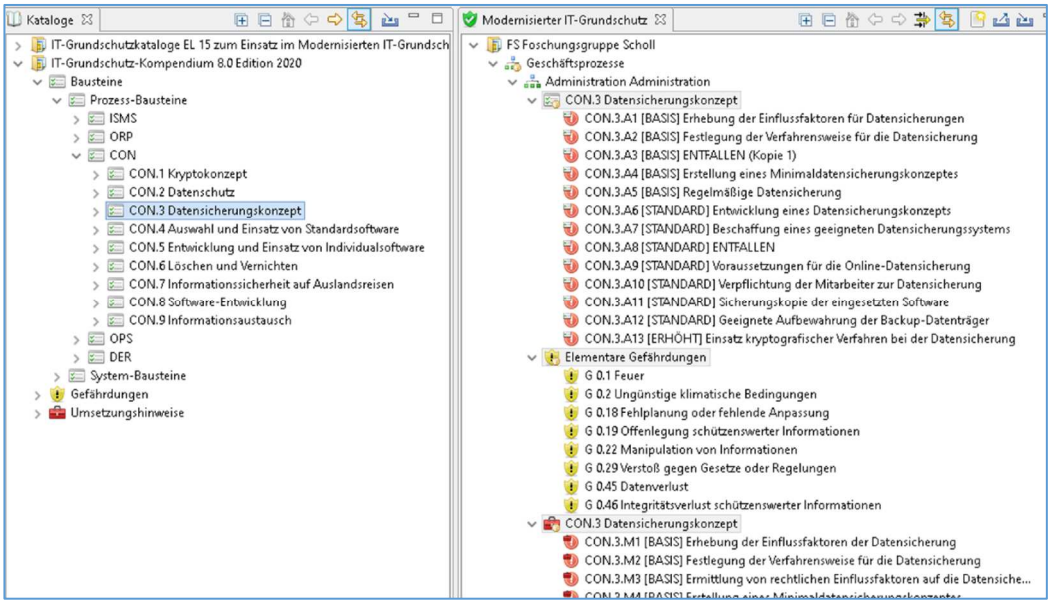


Fig. 60 The administration process is modeled with the CON.3 module. This means that the process module CON.3 is assigned to the administration process of the information domain FS—i.e., it is moved via drag and drop from the left side to the right side to the appropriate screen position.

4. Next, model APP.3.1 web applications on the "NextCloud web server" application and APP.3.2 web server on the "TEDS web server" application (fig. 61).

It can then be seen in fig. 61 that the APP 3.2 system module has not yet been completed or is incomplete, since no measures or instructions for action have yet been entered by the BSI in the *IT-Grundschutz Compendium*, version 8.0, 2020 edition.

The background to the following exercise is as follows: after searching in the *IT-Grundschutz Compendium* and by using the relevant implementation information, we engaged in talks with the responsible parties to clarify technical concerns.

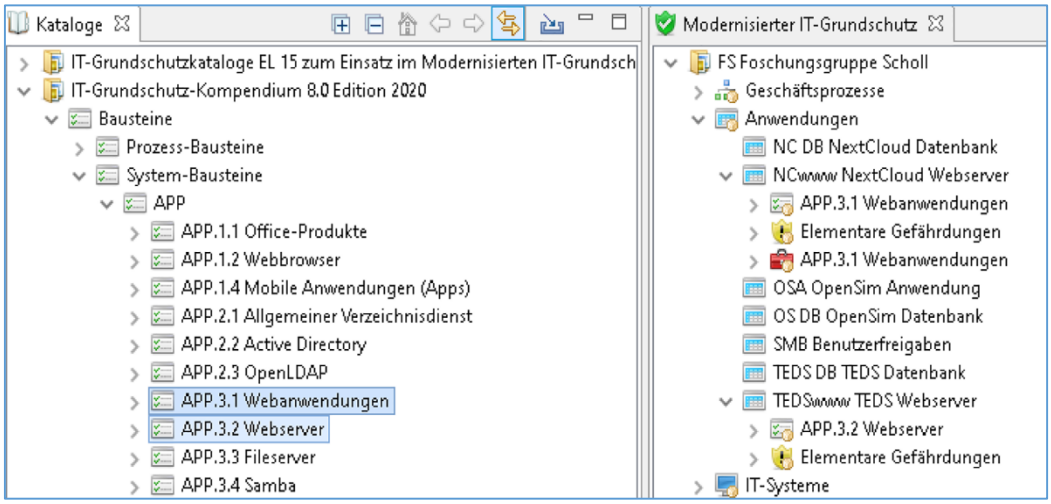


Fig. 61 Modeling using the APP.3.1 and APP.3.2: APP.3.1 system modules is assigned to the "NextCloud web server" application in the information domain. The system module APP.3.2 is assigned to the "TEDS web server" application in the information domain created for the exercise.

We can determine that the basic requirement APP.3.2.A5 "Authentication (B)" is perfectly fulfilled by the APP.3.1.M1 measure "Authentication" for web applications. Based on this, we create the APP.3.2 web server module for the "TEDS web server" (fig. 62).

5. Right-click on the "TEDS web server" and create a new group "APP.3.2 web server" (fig. 62):

Fig. 62 Create a new measure group "APP.3.2 web server" for the "TEDS web server."

6. Afterwards the individual measures can be copied from the *IT-Grundschutz Compendium* (fig. 63):

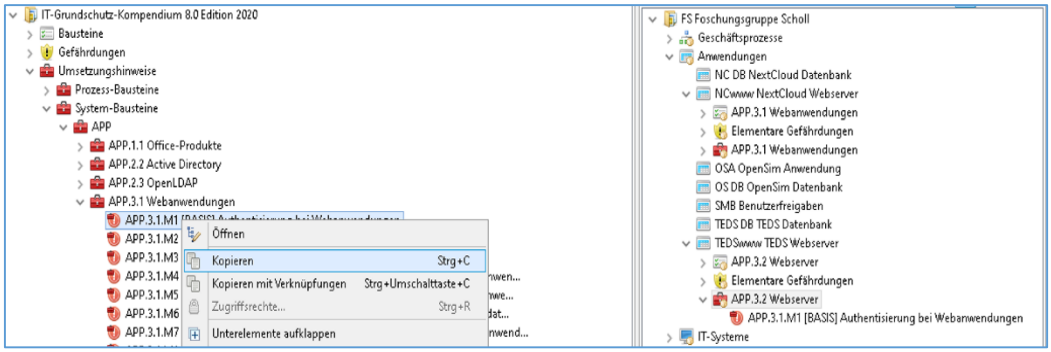


Fig. 63 Measure APP.3.1.M1 is copied into the individual measure group: right-click on the measure—copy. Right-click on the measure group—insert.

In order to fulfill the APP.3.2.A5 authentication requirement, a corresponding link must be created in the next step of the exercise (fig. 64).

7. Create a corresponding link analogous to fig. 64:

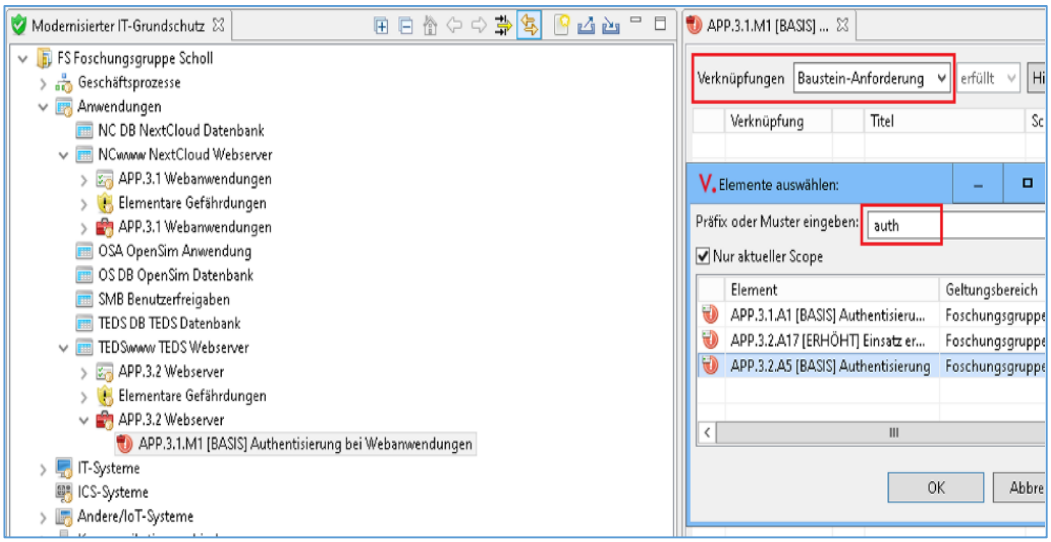


Fig. 64 The APP.3.1.M1 measure is linked to the APP.3.2.A5 module requirement (i.e., it is "modeled").

In order to achieve correct modeling, these steps must be carried out for each module requirement, no matter if it is a basic requirement for basic protection (B) or an additional standard requirement for standard protection (S). If the deviations are larger and there are no measures that can be copied or adapted from the old IT-Grundschutz catalogs or in the new *IT-Grundschutz Compendium*, a risk analysis is required, along with the creation of individual measures. For the next steps, the modeling of the server room must also be linked manually, since there are no measures in the updated IT- Grundschutz approach at the time of our exercise (April 2020).

8. Check the screen with the following catalog view (see fig. 65):

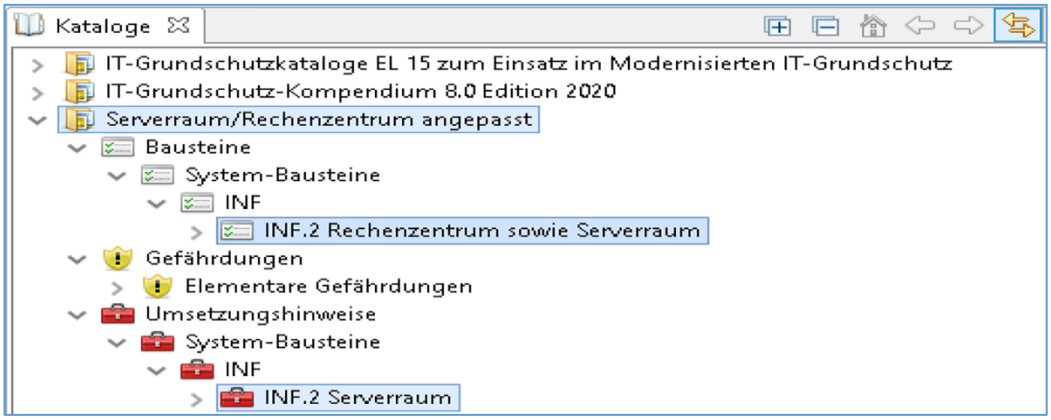


Fig. 65 Completed module INF.2 (data center and server room) for the exercise.

As there are no implementation notes or measures for the *server room* available in the current *IT-Grundschutz Compendium* (April 2020), this object was modeled using measures from the old IT-Grundschutz protection catalogs. In this case we speak of *hybrid modeling* (using a mix of the old catalogs and the new compendium). However, the BSI migration tables can be found in the migration guide [16] to help you locate suitable measures.

In general, in the absence of measures to reduce the risks to the information domain, the current compendium should be searched before old measures from the protection catalogs are used. After this, and only then, should *individual* measures be created, since this work can usually only be done by the relevant specialist and takes a considerable amount of time. The modeling of our information domain is now complete.

3.5 The IT-Grundschutz check (part 1)

An IT-Grundschutz check is a target-actual comparison, in which a check is made of the extent to which the selected information domain fulfills the relevant security requirements. According to BSI Standard 200-2 [17] the following four evaluation results can occur:

- "Not necessary," meaning that the fulfillment of the particular requirement is not relevant in the present application scenario;
- "Yes," meaning that the module's requirements have been fully and effectively met;
- "Partially," meaning that some aspects of the security requirements have been met;
- "No," meaning that the security requirements from the modules in the *IT-Grundschutz Compendium* have essentially not been met.

For this part of the tool-based exercise, we will, from now on, only concentrate on the defined *server room* of our information domain FS (see fig. 16).

For the IT-Grundschutz check in the exercise, we assume a (simulated) survey of all those responsible for the target-actual comparison. The following status information on these module requirements was recorded as an example:

- INF.2.A2 Creation of fire zones
  - M 1.47 Discrete fire zone
    Discrete fire zone is present (implemented).
- INF.2.A8 Use of a fire alarm system
  - M 1.75 Fire detection in buildings
    Fire detectors are available and regular checks are carried out (implemented) by the fire protection officer.

  - M 1.47 Discrete fire section
    See above (implemented).
  - M 1.48 Fire alarm system in the data center
    There is a fire alarm system, but it is not linked to the air conditioning (partially implemented).
- INF.2.A11 Automated monitoring of the infrastructure
  - M 1.31 Remote display of faults
    There is no remote display of faults (not implemented).
- INF.2.A15 Surge protection device
  - M 1.25 Surge protection
    This is already included in the central UPS systems (not necessary).

1. Open the respective measures in the tool and enter the implementation status for all six measures. Also complete the “Standard” approach. Note the change in the symbol’s color for all the measures that have been processed, depending on the implementation status (fig. 66):

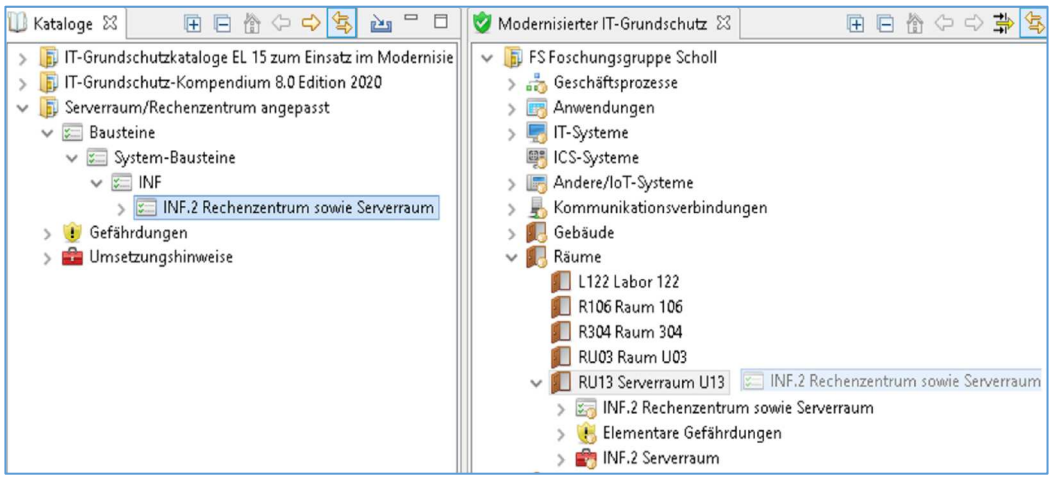


Fig. 66 Setting up the five sample results from the IT-Grundschutz check for the server room of the information domain created for the exercise.

2. After all the assumptions for the measures have been entered, the module requirements must be checked. Here, the implementation status of the measures (also for several measures) is derived from the links and marked with symbols. Compare the requirements with the linked measures according to figs. 67 and 68.

The IT-Grundschutz check has been completed for the example. Unfortunately, we cannot show the exact content control of the respective measures in this book. Since ISOs do not have to be experts in the particular area relating to the measure or process, it is customary to turn to the relevant specialists in the institution. Those responsible can be linked directly to the measures using the link option in the tool. Documents and further information can also be stored.

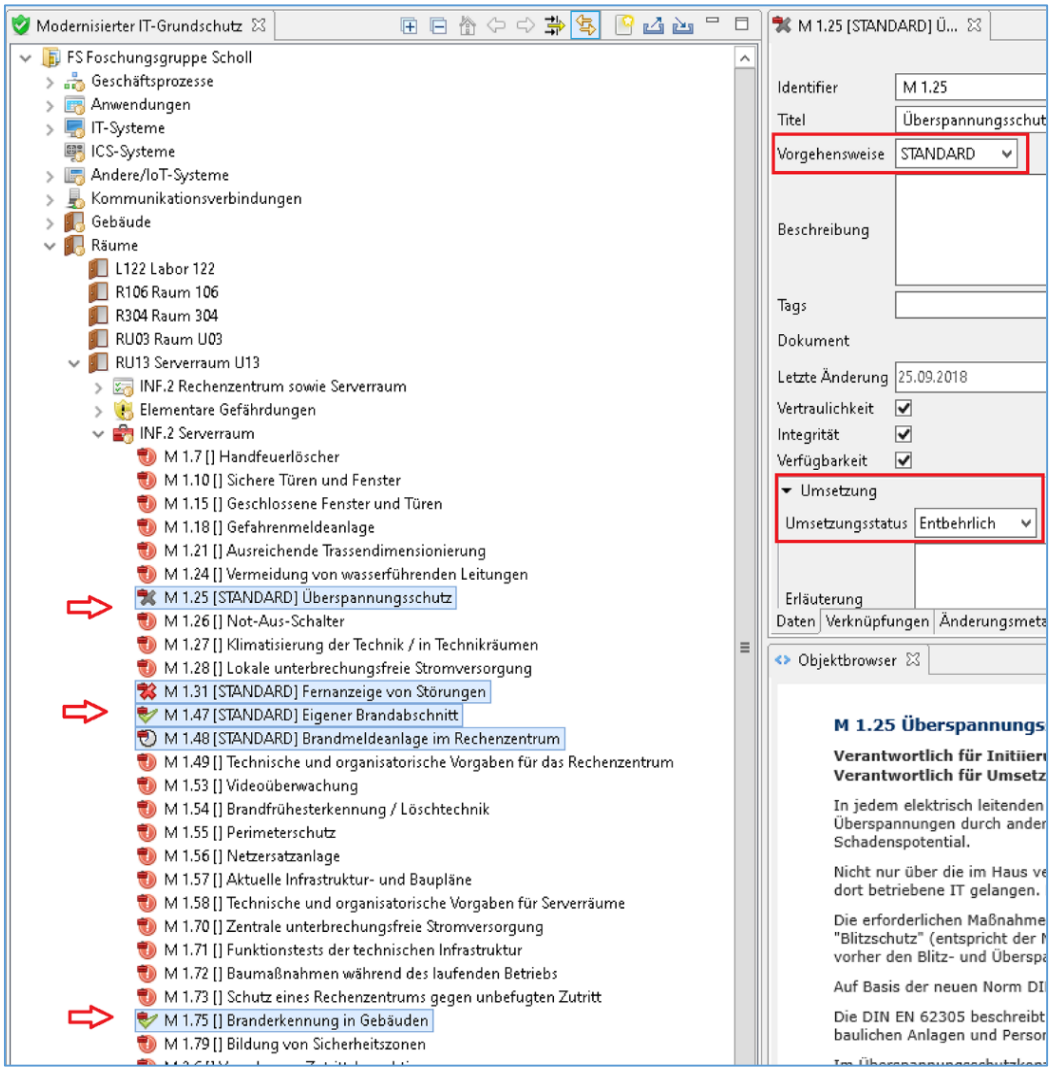


Fig. 67 Setting up the six sample survey results for IT-Grundschutz check I. Readers may create plausible settings in their own exercise tool example.

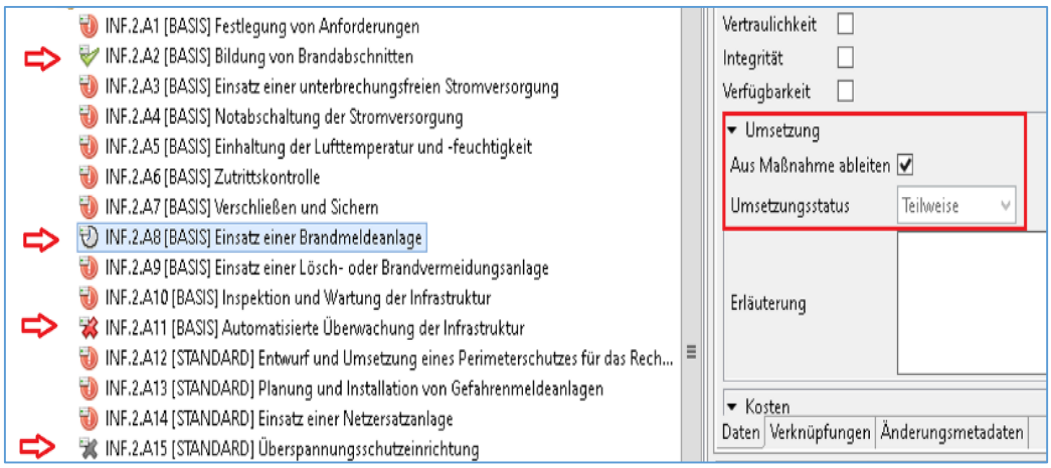


Fig. 68 Setting up the specific implementation status for the information domain in the exercise. Readers may create plausible settings in their own exercise tool example.

With the IT-Grundschutz check, the security measures already implemented are compared with the requirements of the *IT-Grundschutz Compendium* in order to identify the security level achieved and to point out opportunities for improvement. The check is an efficient instrument for answering questions such as:

1. Are the information and information technology in the defined information system sufficiently protected?
2. What else must/should be done?

Readers may complete this IT baseline protection check in their own exercise.

3.6 Realization planning I

Realization planning takes place after the IT-Grundschutz check has been completed. In this case, only the estimated costs and efforts play a role with regard to the tool used. The links during the check should already have defined the responsible people and their tasks.

The tool used does not pass the costs on through the links to the measures in the requirement modules. Before making the general settings, thought must be given to whether the costs are assigned to the individual measures or the requirement modules.

Since only a few implementation instructions or measures are considered in our exercise, we will look at the following three measures as an example of implementation:

- M 1.75 Fire detection in buildings
  - Fixed costs: 45,000 euros
  - Material costs: 130 euros per month.
- M 1.31 Remote display of faults
  - Fixed costs: 25,000 euros
  - Material costs: 50 euros per month.
- M 1.48 Fire alarm system in the data center
  - Fixed costs: 20,000 euros
  - Material costs: 150 euros per month.

Readers may supplement their own exercise independently.

1. Fill in the costs of the individual measures in your exercise tool as per fig. 69 below.

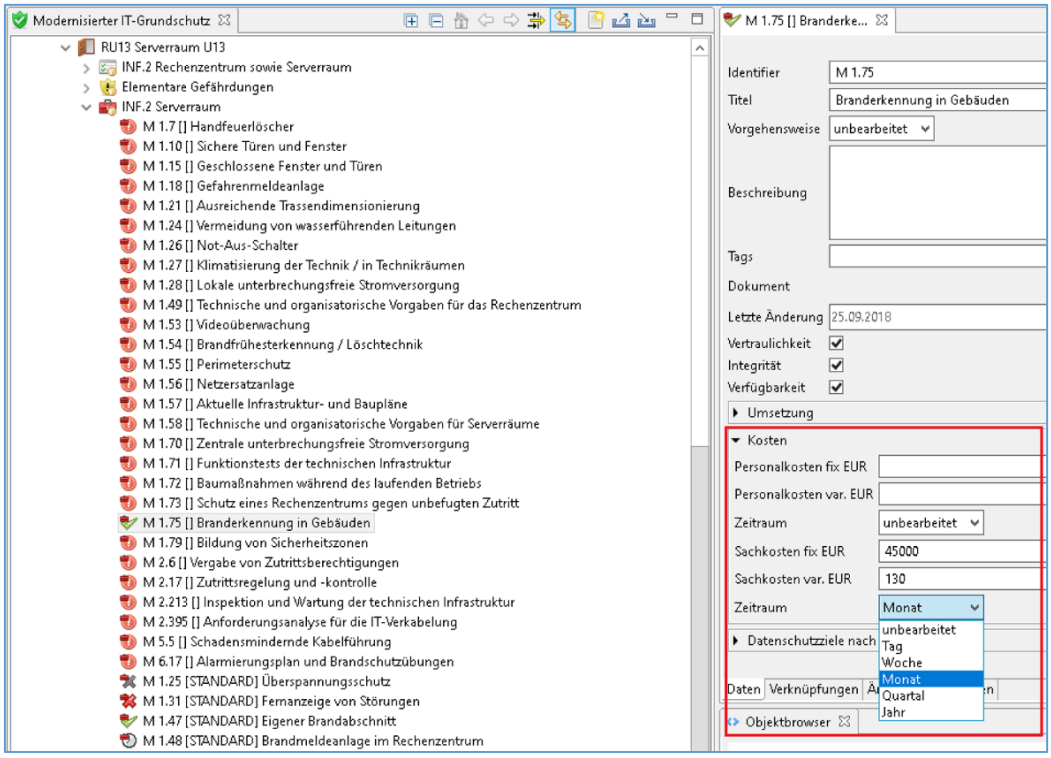


Fig. 69 Completion of the costs for M 1.75 "Fire detection in buildings".

2. In addition, the HRZ must be defined as being responsible for the implementation of the measures. This takes the form of a link between the measure and the HRZ, as shown in fig. 70:

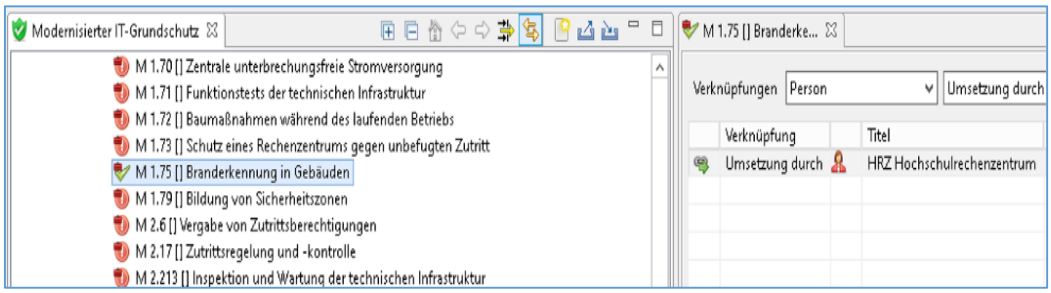


*Fig. 70 Linking the HRZ as a group responsible for implementation. **Note**: In adopting a nuanced approach, other individuals can be defined to take on overall responsibility and to cover IT revision. In reality, the situation is usually more complex. In the tool, it is possible to separate implementation and control, as recommended by the BSI.*

3.7 Generating a report

With all the sample settings and links now completed, we can briefly discuss the creation of a report. This step in the exercise should illustrate how the data for documentation, revision, or testing can be prepared from the database behind the tool.

Please note that it is not possible to generate a report in the free version of the *verinice* tool: for this, you will need the purchased version of the software.

Create a report

- You can access the reports via the menu “File” → “Generate report.” Generate the baseline protection (“A4 Grundschutz-Check”) and realization plan (“A6 Realisierungsplan”) reports as PDFs as per fig. 71:

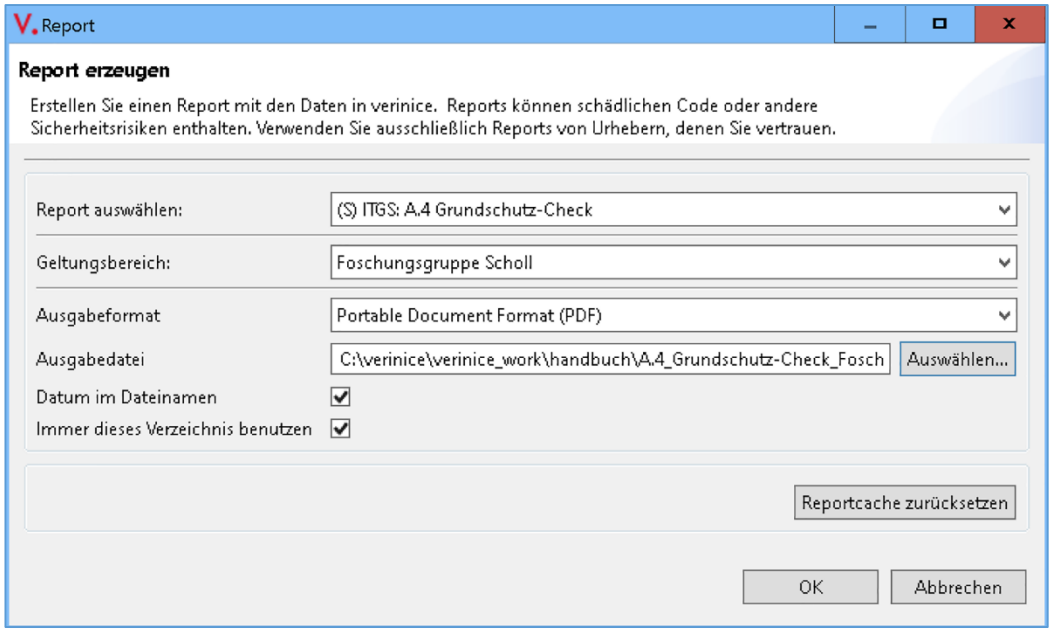


Fig. 71 Generation of reports in line with the updated IT-Grundschutz in the tool verinice for the information domain created in the exercise: Research Group Scholl (“FS Forschungsgruppe Scholl”).

As only some data was entered in the tool for the server room as part of this sample exercise, the reports in the remaining areas are relatively empty. However, you can see the tree-like structure, which allows the responsible persons to map out the implementation of security measures or deliver the IT-Grundschutz check. The example opposite shows the report INF.2.A8 “Use of a fire alarm system” from the IT-Grundschutz check (fig. 72).

INF.2.A8	Einsatz einer Brandmeldeanlage	
Beschreibung:		
Hauptverantwortlicher:		
Verantwortlicher:		
Umsetzung durch:		Umsetzung bis:
Umsetzungsstatus:	Teilweise	
Umsetzungserläuterung:		
M 1.48	Brandmeldeanlage im Rechenzentrum	
Beschreibung:		
Umsetzung durch	Hochschulrechenzentrum	Umsetzung bis:
Umsetzungsstatus:	Teilweise	
Umsetzungserläuterung:		
M 1.47	Eigener Brandabschnitt	
Beschreibung:		
Umsetzung durch	Hochschulrechenzentrum	Umsetzung bis:
Umsetzungsstatus:	Ja	
Umsetzungserläuterung:		
M 1.75	Branderkennung in Gebäuden	
Beschreibung:		
Umsetzung durch	Hochschulrechenzentrum	Umsetzung bis:
Umsetzungsstatus:	Ja	
Umsetzungserläuterung:		

Fig. 72 Report INF.2.A8 “Use of a fire alarm system”.

3.8 Risk analysis and consolidation

In chapter 3.3 of this tool-based exercise, which focused on determining the protection needs of the information domain, we argued that the server room had a high protection requirement with regard to confidentiality. We have also established that it is impossible to comply with this high protection requirement in a public university building, so that the maximum principle is violated in this case. It is therefore necessary to give special attention to the server room by conducting a risk analysis.

Before a risk analysis can be initiated in the tool, the parameters of the risk analysis for the information domain must be clarified and defined with the ISM team and all the other responsible parties using the six damage scenarios (see chapter 2.2). This includes

- the risk matrix,
- the risk categories,
- the categories of damage effects, and
- the frequency of occurrence of events.

As explained in chapter 2, BSI Standard 200-3 [18] provides general information on this procedure, which has been adopted in the *verinice* tool (see fig. 73). These definitions must be checked and stipulated by each institution on an organization-specific basis. However, no changes are made to the definitions for this exercise.

1. Open the information domain with a double click in the tool (fig. 73) and look at the four tabs Risk Matrix (in German: *Risikomatrix*), Risk Category (*Risikokategorie*), Impact (*Auswirkung*), and Frequency of Occurrence (*Eintrittshäufigkeit*):

Fig. 73 Risk definition for the information domain in the tool (exercise in German).

In this step, we recommend a risk comparison of the server room and the publicly accessible university building: because, in the example, we breached the maximum principle for the building “Haus 100” in the exercise, it now makes sense to model H100 as a general building (see fig. 74). As explained in chapter 2, the updated IT-Grundschutz uses a total of forty-seven elementary threats for that.

2. Model H100 separately as a general building as per IT-Grundschutz module INF.1 (“INF.1 Allgemeines Gebäude”) (see fig. 74):

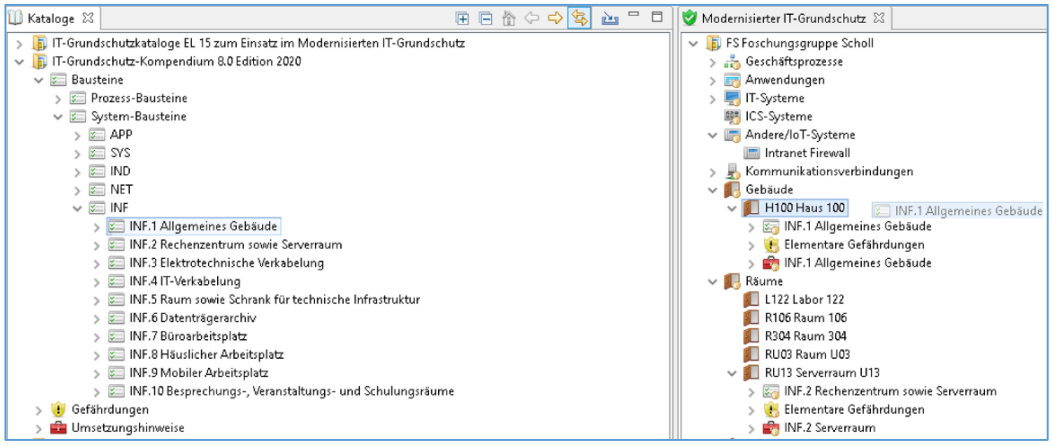


Fig. 74 Modeling of “Haus 100” as a general building (“INF.1 Allgemeines Gebäude”) in line with the IT-Grundschutz module INF.1.

3. This step involves a preliminary analysis of the existing threats. Open the elementary threats both in H100 and in the server room and compare them.

In practice, we recommend initiating a discussion between those responsible for the server room and those responsible for the building to compare these elementary threats. For this purpose, all the requirements and measures from both modules must be looked at together in order to be able to make a sound assessment of threats that have not been sufficiently addressed or additional threats to the server room. Measures are to be derived from this discussion in consultation with the top management. For the exercise, we assume that this process of coordination has produced the following result (see table 2, figs. 10 and 76):

- **G 0.4** Dirt, dust, corrosion (insufficiently addressed threats)
  Frequency of occurrence *medium* (“mittel”), impact *significant* (“beträchtlich”)
- **G 0.9** Failure or malfunction of communication networks (additional threat)
  Frequency of occurrence *rarely* (“selten”), impact *limited* (“begrenzt”)
- **G 0.10** Failure or malfunction of supply networks (insufficiently addressed threats)
  Frequency of occurrence *rarely* (“selten”), impact *limited* (“begrenzt”)
- **G 0.18** Poor planning or lack of adjustment (to be addressed separately)
  Frequency of occurrence *often* (“häufig”), impact *significant* (“beträchtlich”)
- **G 1.18** Failure of a building (e.g., in the event of an attack or sabotage based on the older BSI standards 100-2/100-3 and the BSI catalogs)
  Frequency of occurrence *rarely* (“selten”), impact *significant* (“beträchtlich”).

For the exercise, we think it makes sense to model the risk analysis in a *hybrid* way, too. This means working in general with the new BSI standards 200-2 and 200-3, while using the old BSI Standards 100-2 and 100-3 for the defined threat G 1.18. The alternative to this hybrid modeling is to create your own new, individual threats and requirements.

4. To depict the facts described in the tool, the risk analysis for the server room must first be defined as per fig. 75—i.e., you should enter a description of the reason for carrying out the risk analysis.

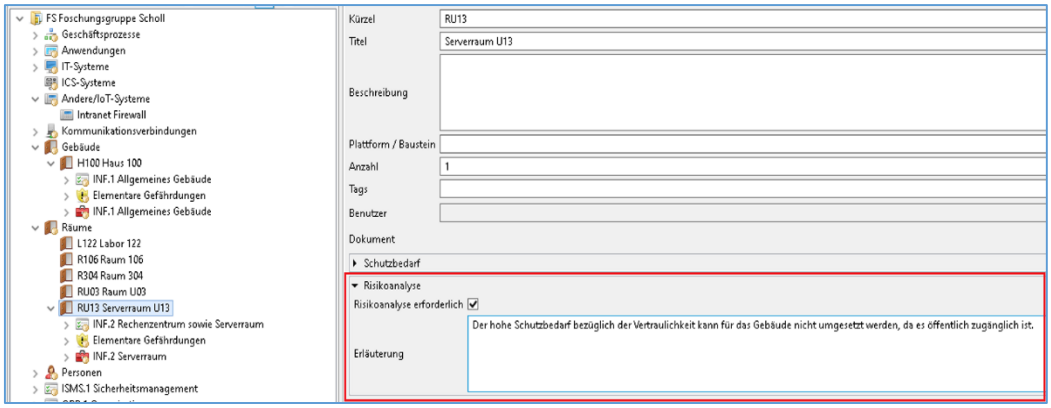


Fig. 75 Enter the reason for the risk analysis of the server room in the tool (here in German).

5. Add the additional threats to the server room in a separate risk group. This is done with a right click on the server room U13 with the abbreviation RU13 (see fig. 35: “RU13 Serverraum U13”). Then copy the additional threats both from the *IT-Grundschutz Compendium* and from the older BSI catalog to this new risk group (fig. 76).

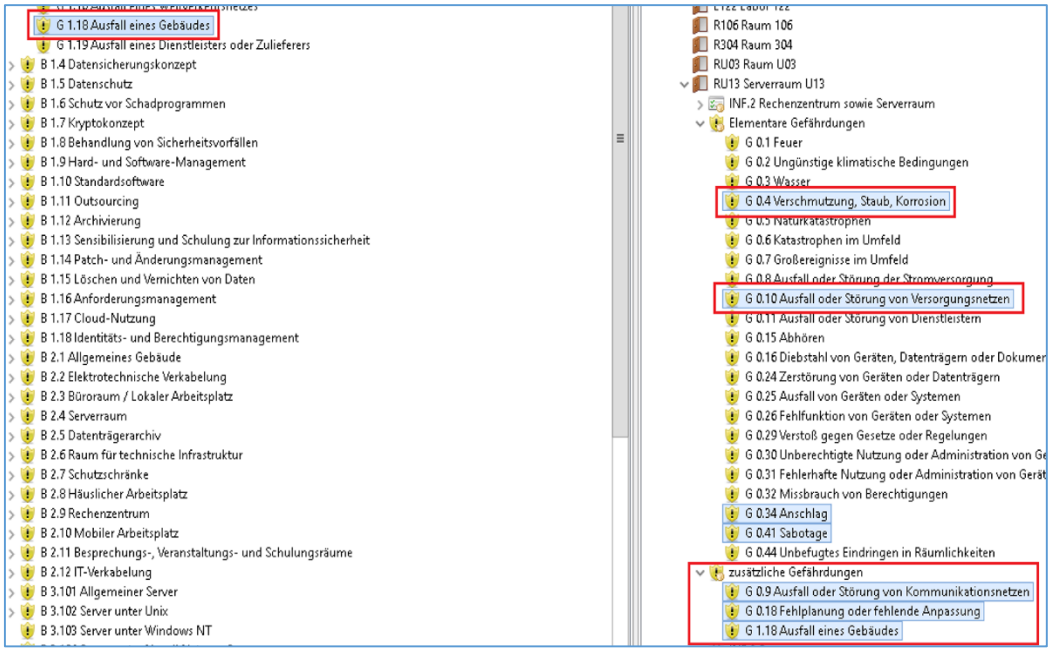


Fig. 76 Sample overview of threats for the server room in the information domain in the exercise.

6. The next step is to classify the risks or threats in terms of the question “What are the dangers if the risk is not addressed?” Complete the area “Risk without additional measures” (in German: “Risiko ohne zusätzliche Maßnahmen”) for all the threats listed (see fig. 77). Note the automatic risk determination using the previously defined risk matrix.

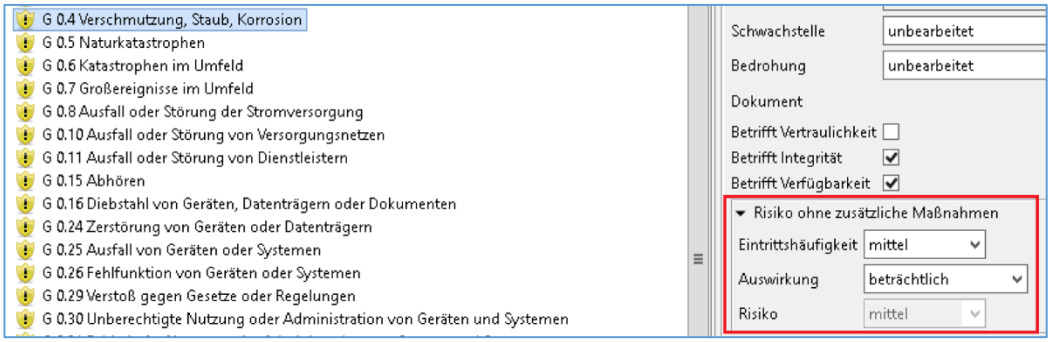


*Fig. 77 Assessment of the risk in the tool (on the right) for the elementary threat **G 0.4** Dirt, dust, corrosion (on the left: “G 0.4 Verschmutzung, Staub, Korrosion”) if no measures were taken.*

7. In order to display an overview of the threats (see fig. 78), the standard view of the tool must be changed. To do this, go to the Edit menu (in German: “Bearbeiten”), Settings (“Einstellungen”), General settings (“Allgemeine Einstellungen”) and activate the option to show the icon overlay for risk analysis values as per BSI IT-Standard 200-3 (“Zeige Icon-Overlay für Risikoanalysewerte nach BSI IT-Grundschutz 200-3”).

The colors of the traffic-light system for the ratings that have been entered show the risks as per figs. 73 and 78 as defined in the risk matrix. In the current view in your exercise setup, however, the color red should be missing, because our exercise excludes the risk category “very high.” It is now important to address the risks. In order to maintain an overview, two new groups are required, which are created below (see fig. 79).

8. For a better overview, create a new module INF.2 for the additional risk requirements (in German: “INF.2 zusätzliche Risikoanforderungen”) and a new measures group INF-2 for the additional measures (“INF-2 zusätzliche Maßnahmen”) of the risk analysis. This is done by right-clicking on the *RU13 server room* (see fig. 79).

According to BSI Standard 200-3, there are the following four options for addressing risks (see chapter 2):

- Risk **avoidance**—e.g., by changing the field of application
- Risk **reduction**—e.g., by implementing further security measures
- Risk **transfer**—e.g., by taking out appropriate insurance
- Risk **acceptance**—e.g., by accepting the residual risk (no action taken).

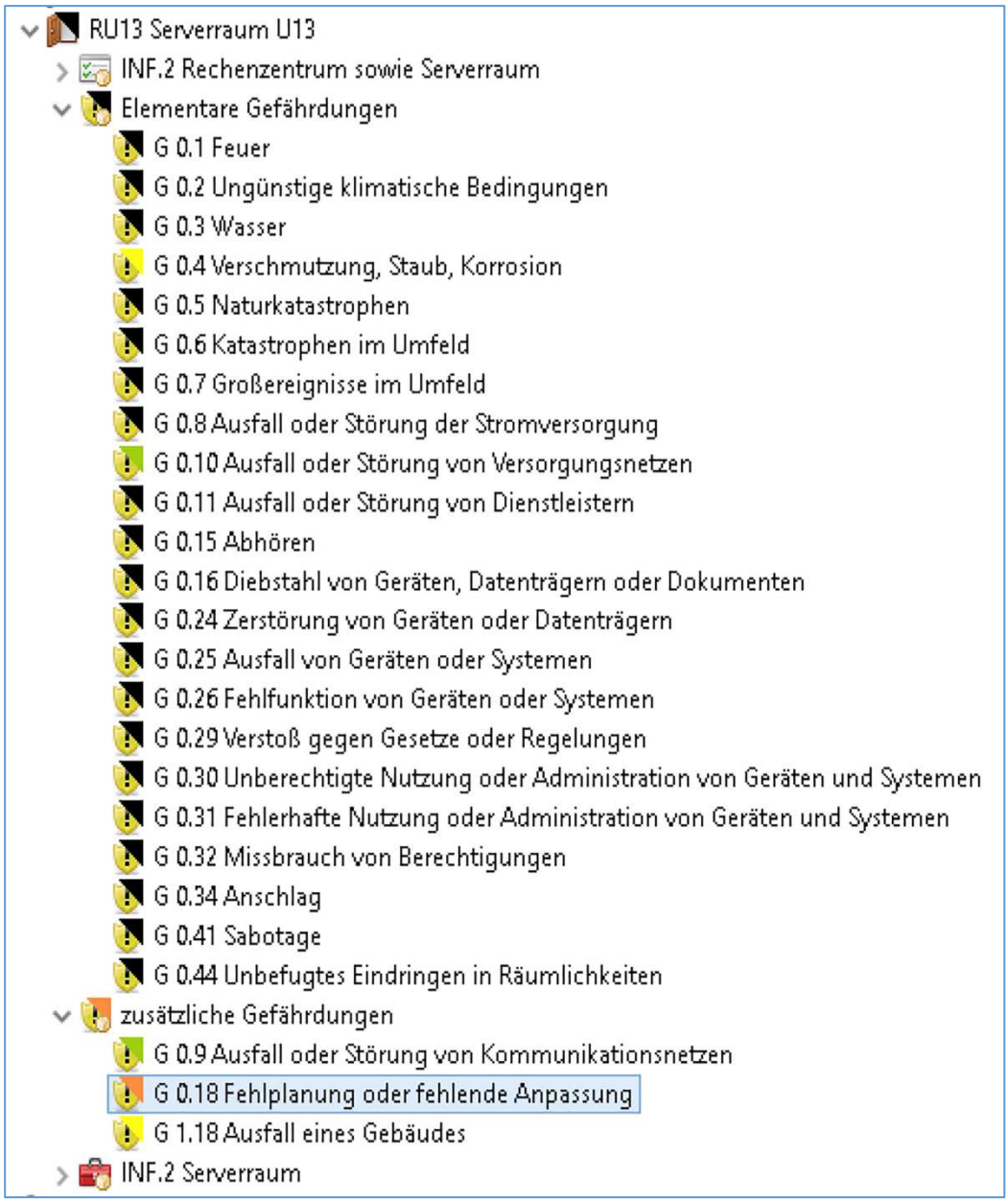


Fig. 78 Traffic-light system for risks relating to the server room in the information domain FS in the exercise.

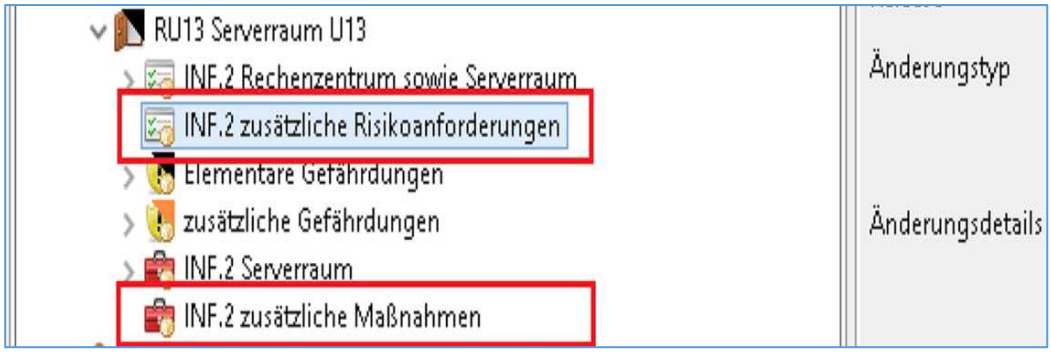


Fig. 79 To provide a better overview of the modeling of measures from the risk analysis, the new module group "INF.2 zusätzliche Risikoanforderungen" and the new measures group "INF-2 zusätzliche Maßnahmen" are created in the tool.

For the exercise, we assume the following (simulated) results for the coordination between the responsible persons, the administrators, the building services, and the top management:

- **G 0.4** Dirt, dust, corrosion (insufficient)
  Risk **reduction** through further measures:
  - INF.6.M3 Protection against dust and other dirt (new).
- **G 0.9** Failure or malfunction of communication networks
  Risk **reduction** through further measures:
  - INF.4.M1 Selection of suitable cable types (new).
  - INF.4.M8 Fire protection of routes (new).
- **G 0.10** Failure or malfunction of supply networks (insufficient)
  Risk **transfer** to the relevant provider
  - Contract extension (new).
- **G 0.18** Poor planning or lack of adjustment (new)
  Risk **acceptance** of the top management
  - Management assumes responsibility for the risk (no action taken).
- **G 1.18** Failure of a building (e.g., in the event of an attack or sabotage as per the older BSI standards 100-2/100-3 and the BSI catalogs)
  Risk **reduction** through further measures:
  - M 1.52 Redundancy, modularity, and scalability in the technical infrastructure as per IT-Grundschutz catalog, category B 2.9 data center (new).

9. Copy the necessary measures and implementation notes from both the IT-Grundschutz catalog and the compendium as per fig. 80:

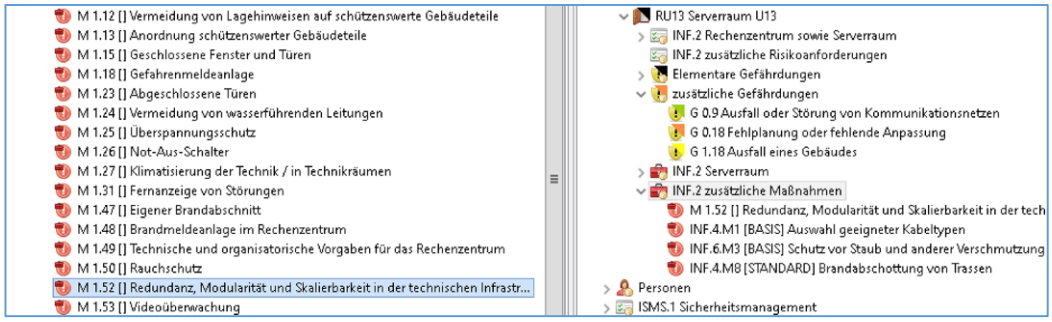


Fig. 80 In this exercise, requirement modules and measures are required for three of the five assumed elementary threats to address the additional risks affecting the server room.

10. Since new elements have been added to the basic structure of our tool-based exercise, the links between these elements need to be added. Use your experience to model the requirements and threats according to fig. 81:

After this additional modeling, the stipulations that were determined to reduce the risk must be implemented (see fig. 82). For the exercise, we assume the following situation after a (simulated) decision by those responsible:

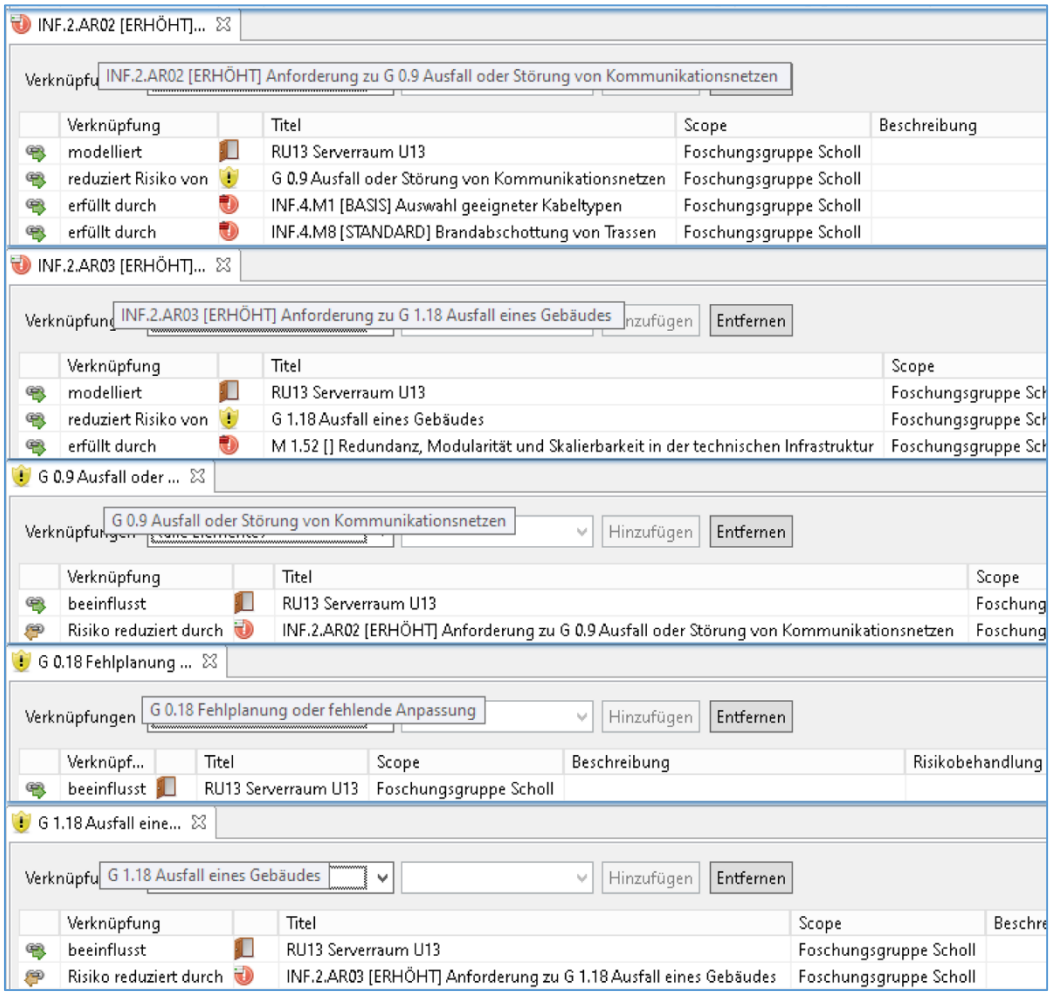


Fig. 81 Modeling of some of the additional measures, threats, and requirement modules.

- **G 0.4** Dirt, dust, corrosion (insufficient)
  - Risk reduction through further measures
  - Frequency of occurrence reduced to *rarely/unlikely* (in German: “selten”)
  - Impact reduced to *limited/medium* (“begrenzt”).
- **G 0.9** Failure or malfunction of communication networks (new)
  - Risk reduction through further measures
  - Frequency of occurrence reduced to *rarely/unlikely* (in German: “selten”)
  - Impact reduced to *negligible/low* (“vernachlässigbar”).
- **G 0.10** Failure or malfunction of supply networks (insufficient)
  - Risk transfer to the respective provider (contracts).
- **G 0.18** Incorrect planning or lack of adjustment (new)
  - Risk acceptance of the management (no action taken to address risk).
- **G 1.18** Failure of a building (e.g., in the event of an attack, sabotage—from the older IT-Grundschutz)
  - Risk reduction through further measures
  - Frequency of occurrence reduced to *rarely/unlikely* (in German: “selten”)
  - Impact reduced to *limited/medium* (“begrenzt”).

- Determine how the risk will be addressed according to the list above and compare your result with fig. 82. As you enter the data, keep an eye on the system of traffic lights relating to the risk assessment and see how the colors gradually change.

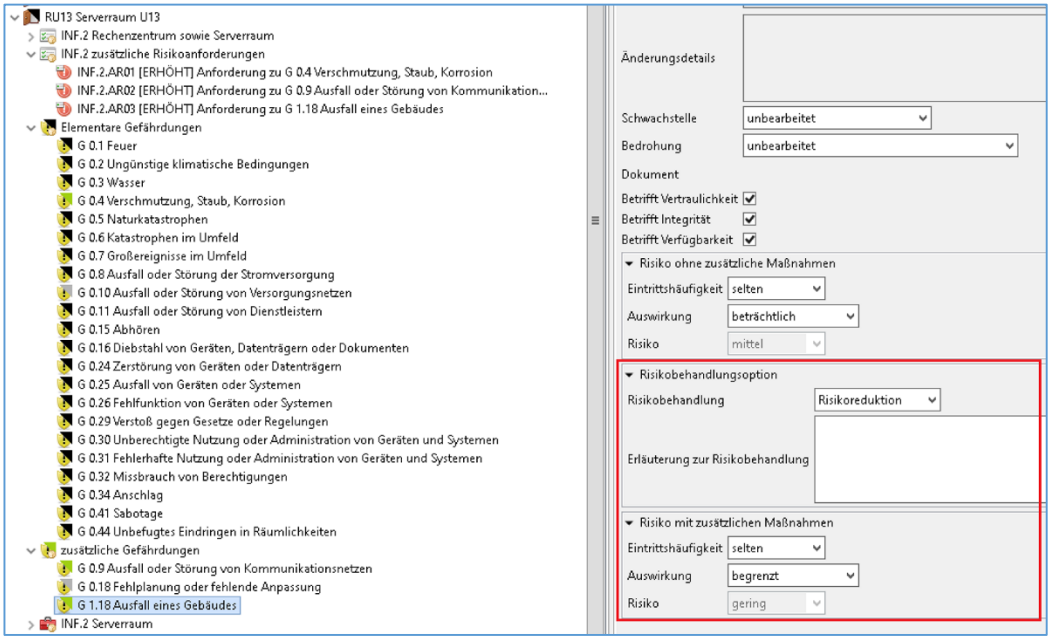


Fig. 82 Result of the action taken to address risk: example of an entry for the threat G 1.18 Failure of a building ("G 1.18 Ausfall eines Gebäudes").

3.9 The IT-Grundschutz check (part 2) and the final implementation planning

After this sample risk assessment, a new (second) IT-Grundschutz check and implementation check need to be performed (see fig. 16). At this point in the exercise, we simply assume that all additional (new) measures have been fully implemented at the time of the IT-Grundschutz check (part 2). We do not consider the measures and requirements from the first IT baseline protection check again. In reality, all the measures would always be checked again during the IT-Grundschutz check (part 2). In addition, we assume that the following costs were incurred in implementing the additional measures:

- INF.6.M3 protection against dust and other dirt (new):
  one-time material cost of 500 euros.
- INF.4.M1 Selection of suitable cable types:
  one-time material cost of 4,000 euros.
- INF.4.M8 Fire insulation of routes:
  one-time material cost of 3,500 euros.
- M 1.52 Redundancy, modularity, and scalability in the technical infrastructure (basic protection catalog category B 2.9 data center):
  one-time material cost of 120,000 euros and monthly costs of 3,000 euros.

1. Set the implementation of the measures with the costs incurred as part of the IT-Grundschutz check (part 2) in the tool and link to the HRZ (entered as “person” in the tool), which will be responsible for the implementation of these measures (see fig. 83). Using the previous modeling, the implementation status of the requirements is derived step by step from the implemented measures as the data is entered.

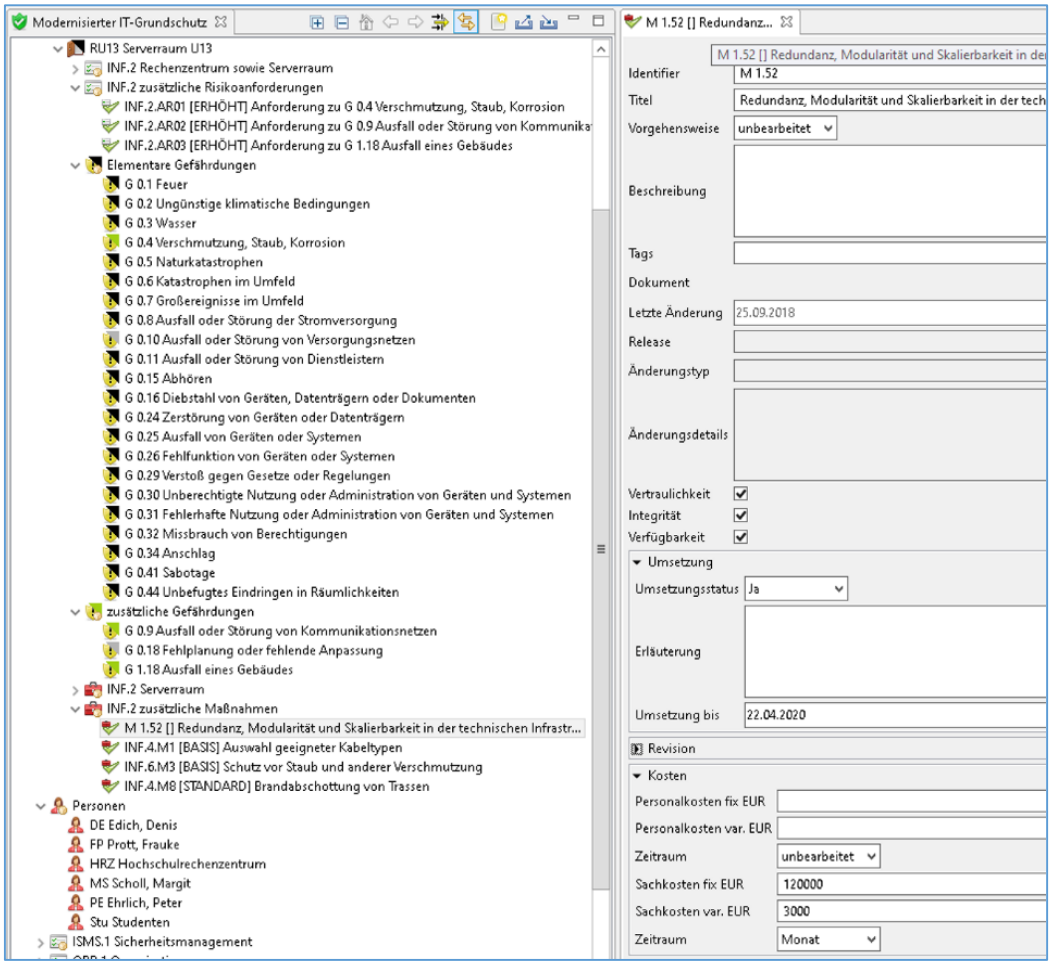


Fig. 83 Example of the IT-Grundschutz check (part 2) relating to the measure M1.51 Redundancy, modularity, and scalability in the technical infrastructure (in German: “M1.51 Redundanz, Modularität und Skalierbarkeit in der technischen Infrastruktur”).

2. Finally, generate the following reports (use chapter 3.7 if necessary):
   - A4 Basic protection check
   - A6 Implementation plan
   - A5 Risk analysis.

3. Compare the results with the reports without risk analysis!

This concludes our practical exercise for tool-based development of an IT security concept for a manageably small information domain. Enjoy your practice time exploring the software!

Please test yourselves with the following questions and comments for chapter 3:

- Can you identify the *sequence of steps* for the (tool-based) development of an IS concept for a defined information domain as per the IT-Grundschutz approach?

- Explain the term “grouping.”

- Which four categories does the tool *verinice* show to describe the protection requirements of objects in the information domain?

- What are the consequences of the “maximum principle”?

- What does the “distributive effect” mean?

- Explain the importance of the “cumulative effect.”

Space for your own comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

4. Sustainable awareness-raising and training geared to specific target groups as the basis for ensuring security measures are accepted

IT-Grundschutz primarily refers to the three basic IS values of confidentiality, integrity, and availability, which are to be made clear to all managers and employees through awareness-raising and training measures. Depending on the institution and IT application scenario, other protection goals must also be considered (see fig. 84). For example, authenticity refers to the property that guarantees that an IT component, application, or person who presents themselves is actually who they claim to be. The authenticity check therefore means ensuring the actual source of information and is particularly important for electronic signatures that replace the classic signature with cryptographic methods. In addition, cryptographic procedures are designed to ensure the confidentiality and integrity of information.

Fig. 84 Author's flipchart diagram of the three basic values of IS and other protection goals depending on the institution and IT application scenario: Availability (in German: Verfügbarkeit), Integrity (Integrität), Confidentiality (Vertraulichkeit), Authenticity (Authentizität), Non-contestability (Nichtabstreitbarkeit), Commitment (Verbindlichkeit), Compliance with laws, standards, and norms (Gesetze, Standards und Normen), and Reliability (Zuverlässigkeit).

Non-contestability and commitment are further protection goals that seek greater legal security using technical tools. Non-contestability refers to the ability to verify that information has been sent or received, as is the case, for example, with De-Mail. The commitment is a combination of authenticity and non-deniability.

In addition, managers and employees must comply with the laws that are important for their work, as well as the norms and standards of IS. Reliability in this context means the ability of IT components to function without failure and includes their quality in terms of correctness and robustness. Reliability therefore also influences the availability of technology and services. The basic values of IS, further protection goals, relevant information from the norms and standards for IS, or from the *IT Grundschutz Compendium*, are to be made clear to the managers and all employees for their specific work and tasks. In the BSI compendium, you can find the process module *ORP Organization and staff* and the specific component *ORP.3 Sensitization and training* [27], which describes how an effective awareness-raising and training program on IS can be set up and maintained in an institution.

The motivation is to understand that employees are key to successfully achieving a high level of institutional IS. The aim of such a program is to refine employees' perception of security risks and to provide them with the necessary knowledge and skills to support security-conscious behavior [27]. Managers and employees must be made aware of the relevant threats to an institution's business processes. They should know how such threats can impact the organization, what is expected of them with regard to IS, and how they should react in security-critical situations.

In essence, the ISO is responsible for ensuring that all requirements are met and checked in accordance with the security concept that has been defined. As far as an institution's program for awareness raising and training is concerned, other responsible persons must be included for its implementation, such as IT operations, top management, the human resources department, and senior officers [27].

According to the ORP.3 module, employees must be made aware of the following threats [27]:

- Insufficient knowledge of IS regulations (policy, guidelines)
- Insufficient awareness of IS
- Ineffective awareness raising and training activities, possibly caused by
  - lack of management support
  - unclear goals or poor planning
  - lack of success control
  - lack of continuity
  - insufficient financial or human resources
  - inadequate training of employees on security functions
- Undetected security incidents
- Non-observance of safety measures or carelessness
- Lack of acceptance of IS requirements—for example, through
  - a lack of security culture in the institution
  - a lack of role modeling by the management
  - inappropriate security requirements
  - the installation of particular hardware or software equipment as a status symbol
- Social engineering, in which the attackers skillfully manipulate employees for illegal purposes, often in a multistage procedure.

Of the forty-seven basic threats cited, the following are explicitly mentioned in ORP.3 [27]:

- G 0.14 Espionage (spying on information)
- G 0.15 Line tapping
- G 0.19 Disclosure of information that should be protected
- G 0.24 Destruction of devices or data media

- G 0.29 Violation of laws or contracts
- G 0.30 Unauthorized use or administration of devices and systems
- G 0.31 Incorrect use or administration of devices and systems
- G 0.32 Misuse of authorizations
- G 0.36 Identity theft
- G 0.37 Repudiation of actions
- G 0.38 Misuse of personal data
- G 0.42 Social engineering
- G 0.45 Loss of data
- G 0.46 Loss of integrity of information that should be protected.

What requirements have to be met according to the IT-Grundschutz module ORP.3 and who is responsible? The following three requirements can be summarized as a *basic protection approach* (B; see [27]):

- ORP.3.A1 (B): The management of the institution must be made sufficiently conscious of security issues by the ISO, and the support of the top management for an awareness-raising and training program must be ensured. In addition, the top management must support the training measures for employees, all superiors must act as role models, and the managers must implement the security requirements and instruct the employees on their compliance.
- ORP.3.A2 (B): In the institution, contact persons must be put in place for simple or complex security questions, and these persons must be known to all employees.
- ORP.3.A3 (B): All employees and external users must be instructed in the safe use of systems and services and given an awareness of this as it relates to their work. IT usage requires that binding, comprehensible, and current guidelines be available and properly communicated.

In addition, for the standard protection approach (S) [27], five further requirements are mentioned in the BSI IT-Grundschutz. These can be summarized as follows:

- ORP.3.A4 (S): The awareness-raising and training program should be geared to its specific target group, and it should be regularly checked and updated.
- ORP.3.A5 (S): A target-group analysis should be carried out for the awareness-raising and training program so that the measures can be related to the special requirements and different backgrounds of the group.
- ORP.3.A6 (S): All employees should be trained in line with their IS-related responsibilities and remit, so that they receive all the information and skills they need to be able to implement the applicable security regulations. The content of the IS topics should be planned in a structured manner. ISO should regularly exchange information with other officers and the HR department about the efficiency of the training and further education.

- ORP.3.A7 (S): Since ISOs should be familiar with the IT-Grundschutz, a suitable IT-Grundschutz training should be given with practical examples, which also includes the BSI's online course (see [18]).
- ORP.3.A8 (S): The learning success should be measured and evaluated in relation to target groups. This should lead to improvements in the training. In addition to the ISO, the HR department takes on a central function in fulfilling these requirements.

These eight requirements must be taken into account in an institution's standard protection approach. Based on these requirements and the experience gained from our research projects, we will show specific implementation and training examples in the following chapters.

4.1 Findings from research and training

Employees are an important success factor for IS in an institution, which is why security awareness should be increased and an actual security culture should be established in the institution [27]. Our research [28] showed that technical solutions for IS are necessary to fix certain attack vectors such as viruses, denial-of-service attacks, etc. However, IS is not just about technology [29] [28] and organization but also about people as users of technical systems, who do not always act optimally in line with best practice [30].

A lack of understanding of security issues in connection with the ubiquitous use of computers of all sizes with increasing digitization often makes employees in the literature a "critical factor" in relation to IS. However, as Dark highlighted in 2006, knowledgeable people are better able to prevent IS injuries that result from negligence or accident, as well as those that come from malicious activity and abnormal system behavior [14]. They can respond to incidents efficiently and effectively by promptly reporting them, quarantining problems, and diagnosing and treating them properly [14].

It is now clear that technology solutions alone are not sufficient countermeasures against IS attacks. This is a challenge for the ISM of an institution, since management and behavioral aspects are crucial for the establishment of an ISMS in organizations [15]. The human side of security *must* also be managed to protect organizational resources, including user information and systems [31, 32]. This is particularly evident in the case of social engineering (SE) attacks [33]. People play an important role in successfully deploying IS in today's institutions. The safety behavior of employees is strongly influenced by their *personal risk perception*, and this perception can be changed through awareness raising and training [34].

However, there is no simple linear cause-and-effect relationship between knowledge and attitudes, and certainly not with regard to people's *actual* IS behavior.

A major problem for people seems to be the *use* of IS knowledge in *real situations*. It seems that commitment and personal standards also influence employees' attitudes toward IS. In addition to the proactive role of management, employees have to decide for themselves how they can implement IS in the context of their own specific work tasks. This obviously requires a higher level of skill in terms of information security awareness (ISA). Motivators must also be provided. Research on company IS [2] affirms that psychological factors and subjective norms, coupled with a person's socio-cultural and gender-specific background and the non-linear and complex interactions they engage in, have a great influence on ISA and IS behavior.

According to Beyer et al. (2016), it is necessary to pursue an approach to awareness-raising and training programs that motivates employees to play an active role in the security of the institution [34]. "Employees should understand what to protect, why they should want to protect it, how the organization can help them with this, and how successes and mistakes can be used as opportunities to learn and improve." [34]. The IT-Grundschutz complies with this finding. It requires a cultural change in the institution for IS. This is also addressed by the IT-Grundschutz module *OPR.3* in *part 2.2*: "If employees are insufficiently aware of information security issues, the security culture, security goals, and security strategy of the institution can be endangered." [27]. Our research has found that this change includes a cultural shift within the institution that allows mistakes to be admitted and owned.

Although security communication and security training are intended to align the behavior of employees with the security objectives of the institution, they are not always designed in such a way that this can be achieved (see [34]). The didactic method used for a particular security issue, a change in the teaching method, and communication and interaction are of great importance in awareness-raising and training measures. We should also differentiate between raising awareness ("sensitization") and the in-depth training of employees. A sensitization measure seeks to motivate people to deal with IS issues, create an emotional connection ("emotionalization") so that people understand the importance of the measure, and promote awareness of IS topics.

Training courses are intended to go into depth and offer practice with certain issues. The current scientific literature assumes that the reasons and motives for specific IS behavior are not static but can change over time [35]. The creation of an effective ISA program requires targeted communication, awareness in a specific work context, and training geared to the specific target group. The optimal IS culture must always be carefully defined. But there is no panacea for the development of effective ISA training, because each institution has to define the company-specific security culture that it wants to promote [36]. The secret is that people are involved in the right way so that they can convert learning into tangible actions and new behavior [34].

Research findings show that in addition to the theoretical approach of knowledge transfer, combined with an approach to emotionalization, a systemic communication approach in the form of team-based interactions is required to achieve sustained awareness of information security that includes the intention to protect sensitive information and the appropriate behavior to achieve this [2]. We therefore call the combination of these three approaches *Information Security Awareness Training 3.0* (ISAT 3.0) [37].

This corresponds to the idea that ISA is role-based learning. Users can better understand their roles and responsibilities when using IT systems and electronic services in situation-based learning and exchange. To achieve this, creative techniques as well as digital *and* analog serious games in the field of IS, ISA, and ISAT are becoming increasingly important as learning methods. Our research findings show that an awareness of IS can be achieved relatively simply with analog experience-oriented learning scenarios. Examples from various projects with different target groups are presented in the next chapters.

4.2 Examples from the BAköV awareness campaign *Sicher gewinnt (Security Wins)*

The BAköV, together with the BSI, has been carrying out an awareness-raising campaign called *Sicher gewinnt (Security Wins)* for the federal administrations since 2010 [38]. It is clear from research and training that the more such a campaign is tailored to the specific institution and its target groups, the greater its success. The campaign for the federal administrations thus provides a package of key materials that can be put together by the individual authorities to create the right mix for their specific institution. In addition, a guide and checklists were created to enable ISO to develop, implement, and evaluate an awareness campaign inside the authority they work for. This is summarized in a so-called toolbox with support materials that can be used flexibly, such as moderation cards, flyers, or posters.

Fig. 85 BAköV moderation card set from the awareness campaign "Sicher gewinnt" [38]. The set of moderation cards is offered by the company known_sense [39].

For example, the images in the moderation card set (see fig. 85) can be used for the warm-up phase of a training session. Of course, at the beginning of the training you can also substitute, in general terms, the situation perceived by the participants in their institution, using images that are not governed by copyright restrictions (fig. 86) or by creating your own pictures.

Fig. 86 Images that are not governed by copyright restrictions.

In addition to the pictures, the moderation card set contains green themed cards for IS (see fig. 85), which cover a wide range of security issues. If a specific topic of importance to an institution is still missing, an empty topic card is also available, which can be copied and supplied with the missing term. The first step in our procedure with these extensive thematic maps is that the participants should categorize the IS topics for their institution in the three categories: of *great*, *medium*, or *low* importance. A common outcome of the discussion is that the first step involves clarifying whether the categorization should be based on an ideal state (as it should be in the institution) or on the actual situation. In the next step, we start by focusing exclusively on the topics that have been picked out as of high importance (see fig. 87).

The moderation card set contains cards in yellow with target groups of an institution (fig. 85). If specific target groups are missing, the corresponding blank card can also be copied and labeled accordingly. In the second step, we ask our participants to assign to the target groups the IS topics that are of high importance. The exchange between the participants often shows in a playful way that a matrix structure makes sense for the assignment (see fig. 87).

Fig. 87 Sample result of a discussion between participants in an ISO training course at TH Wildau using the BAköV moderation card set "pictures" from the awareness campaign "Sicher gewinnt" [38]: IS topics with high significance for the institution are assigned to the target groups.

Fig. 88 Sample result of a discussion between participants in an ISO training course at TH Wildau using the BAköV moderation card set "information channels" from the awareness campaign "Sicher gewinnt" [38]: The assessment of which didactic methods work in the institution is geared to three categories: "Works for sure," "May work," "Definitely does not work."

In addition to the sets of cards for “issues” and “target groups,” the BAköV moderation set also consists of cards named “channels,” which relate to the information channels and didactic methods (see fig. 85). Since the topics and the target groups already form a two-dimensional matrix, we would now need a third dimension to assign the methods to the individual topic and the individual target group. In the third step, we thus simplify the assignment and ask, in the case of the individual method, whether it *works*, *may work*, or *definitely does not work* in the institution concerned (see fig. 88).

Of course, the discussion results are always just a snapshot of the participants’ level of knowledge and insight into the process. Using the moderation cards, however, provides an important impulse for awareness raising, namely an interaction of the participants and, above all, the motivation to deal with these issues on an ongoing basis.

We recommend that ISOs make use of such materials to raise the awareness of their colleagues. Another example here is the educational game “Quer durch die Sicherheit” (Across Security), a mixture of quiz and strategy game, which can be played on a table as a board game with figures (see fig. 89) or as a floor game in which people are the figures and move across an oversized playing field.

In addition, the BAköV has also developed a three-hour online course on information security at work as well as a fifteen-minute test “Bundes-Informationssicherheits-Schein (BISS)” (Federal Information Security Certificate). The BISS test is mandatory for all employees in federal administrations. All materials were made accessible to the authorities via the BAköV learning platform [40].

Fig. 89 *The BAköV board game “Quer durch die Sicherheit” from the awareness campaign “Sicher gewinnt” [38] in the TH Wildau version for use in the ISO training. The distribution of the game is done by the company known_sense [39].*

The BSI's implementation module *ORP.3 Awareness and training module* suggests the following thirteen issues for training the target groups in an institution [41]:

- Topic 1: Fundamentals of information security
- Topic 2: Information security at the workplace
- Topic 3: Laws and regulations
- Topic 4: Security concept of the organization
- Topic 5: Risk management
- Topic 6: Information security management
- Topic 7: IT systems
- Topic 8: Operational area
- Topic 9: Technical implementation of security measures
- Topic 10: Emergency preparedness / Business continuity management
- Topic 11: New developments in the IT area
- Topic 12: The business side of information security
- Topic 13: Infrastructure security.

ISOs are advised to use the matrix for a training concept—as contained in the implementation instructions for module *ORP.3* [41]—in which the learning topics can be assigned to the corresponding target groups of an institution. An institution's awareness-raising and training concept must define the content of the relevant topics and assign them specifically to the target groups. Not every target group needs to be informed about a specific topic with the same intensity—however, everyone must know the IS issues for his or her workplace. The *IT-Grundschutz Compendium* (2019 edition) [42] includes the measure *ORP.3.M4: Conception of an awareness-raising and training program for information security*. *ORP.3.M4* refers to a *systematic* awareness-raising measure for all employees, which needs to be anchored in the institution by establishing a continuous process.

Building on this awareness-raising process, employees should receive all the necessary information and skills through supplementary training. The following aspects are particularly important [42]:

- IS awareness raising means that employees are given a keener sense of information security, and their security awareness is trained to meet the requirements of the institution.
- At the beginning of the awareness raising, a goal needs to be defined and further refined in a manner specific to the target group, so that the content can then be developed and the success of the measures, evaluated.
- When defining goals, the focus should be on why IS is important for the institution and its employees.
- The awareness raising measures are to be prepared to suit the particular target group and described as realistically as possible to make them practically relevant.

The following groups are listed in the measure *ORP.3.M5: Analysis of target groups*:

- Management level
- Employees and new hires
- Administrators
- HR department as well as secretary's office, mail room, press area, etc.
- External project staff.

The measure *ORP.3.M6: Planning and implementation of awareness-raising and training courses on information security* [42] elucidates questions and explains the assignment of topics and content to the target groups in a matrix (table 3):

Modul / Zielgruppe	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**
Management level	x	x	x	x		?				?	o	x	x
Employees	x	x	?										
Administrators	x	x	?	x	x		x	x	x	x	x	?	o
Security management	x	x	x	x	x	x	x	x	x	x	x	x	x
Data protection officers	x	x	x	x							x	o	
Infrastructure managers	x	x	x	x	x	o				x		?	x
HR department	?	?	?										
External project staff	?	?	?										
New hires	?	?	?										
N.N.	?	?	?										

Tab. 3 Proposed training modules for each target or function group according to BSI implementation measure "ORP.3.M6" [42]. In the matrix, "x" means "mandatory" and "o," "optional" according to the BSI, while the question mark is our additional suggestion. Our inclusion of N.N. suggests that the table should address the specific target groups for each institution and can be expanded accordingly.

4.3 Examples from the projects *IT-Sicherheit@KMU* and *SecAware4job*

Our first research project, which focused on raising awareness of IS, was funded by the State of Brandenburg in 2013–15. Running under the title "IT security in small and medium-sized enterprises" (abbreviated to IT-Sicherheit@SME), it was divided into two parts with different goals: 1) a flexible infrastructure for the development of mobile trainings for small and medium-sized companies (SMEs); and 2) the implementation of new teaching and learning methods drawn from the area of Business Information Security [2]. To achieve this second aim, the German version of "Security Arena" was acquired from the company known_sense [39]: its content was adapted for TH Wildau, and tested with guests, employees, and students of the university. The adjustments that were made related to the layout and the provision of suitable examples and language for the higher education sector. The Security Arena consisted of ten analog learning scenarios:

- Phishing emails
- Social media networks
- Password hacking
- Social engineering
- Access rights, ID cards, user ID cards
- Security incident management

- Internet services and apps
- Security-on-the-go for business trips
- Clear desk at the workplace
- Privacy policy checklist.

The Security Arena principle is based on what we call the 5-5-5 method for raising awareness: a moderator introduces the specific topic using questions for a maximum of five minutes, the participants play the analog learning scenario interactively for about five minutes, and a maximum of five minutes is allocated for evaluation and feedback. These entertaining learning scenarios, which last approximately fifteen minutes can be set up as a kind of circuit training for any number of learning stations or organized as a competition.

As part of the IT-Security@SME project, we developed a new learning scenario ourselves:

- Secure network architecture (known as "Network Domains," see fig. 90).

This can be used particularly well for the technical training of ISOs and in technical courses at the university. It is used to illustrate the single- or multi-level architecture of secure gateways, and consists of magnetic transparencies and signs symbolizing the individual technical components of networks (see chapter 5.5). Depending on the issue, a team can discuss and try out ideas on the whiteboard to determine how technical components such as routers, switches, access points, application level gateways (ALG), packet filters, and "demilitarized zones" (DMZ) can be meaningfully combined to protect the institution against insecure networks such as the Internet. This discussion promotes and enables ISOs to exchange ideas with administrators of the institution.

The successful use of these experience-oriented analog learning scenarios to raise IS awareness in teaching and training—as well as at events with employees of the university and external guests—encouraged us to conduct further research. In the following project "Information security awareness for job beginners (*SecAware4job*)," which was financed from 2015 to 2017 by the Horst Görtz Foundation (HGS), we

- set up the Security Arena in English at TH Wildau,
- developed further German-language serious games [43], and
- carried out the coding of digital versions covering certain IS topics [44].

This enabled us to raise the IS awareness of students on our English-language courses and to address other IS topics in German in an experience-oriented manner. In addition, the digital versions can be used by participants to check their own progress without any restrictions on time and place. The methodological basis and game-based learning scenarios are presented and explained in the final report of the project [45]. In addition, a description is given of the successful new elective subject "Raising awareness of information security in enterprises," which was introduced for students on part-time business courses, and an outline of its evaluation is given.

Fig. 90 *TH Wildau's analog learning scenario "Secure network architecture/network domains" for use in ISO trainings. It is used to illustrate the single- and multi-level architecture of secure gateways and consists of magnetic transparencies and signs that symbolize the individual technical components of networks. Routers use IP addresses to transport the data packets in the direction of the target network, while switches forward data blocks within a network to devices using hardware addresses. A distinction is made between packet filters and ALG (Application Level Gateways) as the basic components of a firewall. A DMZ ("demilitarized zone") is used to protect other components in a separate, isolated environment (e.g., web server, mail server, guest Wi-Fi, etc.).*

4.4 Examples from the project *Security*

The research project "Gender-sensitive study and vocational orientation for the occupation of security specialist (*Security*)" was funded by the Federal Ministry of Education and Research (BMBF) from September 1, 2017, to December 31, 2019.

The project *Security* aims to get young women and schoolgirls interested in this innovative and forward-looking career as well as in the diverse professional world of information security, in which women are strongly underrepresented [46]. The project developed the brochure "Information Security: A Career with a Future" in German [47], which is available for download on the project website [46]. Moreover, after being presented with an appealing and gender-sensitive picture of this career, including portraits of female role models working in the field, and taking part in an interactive and experience-oriented pilot learning event, female pupils should learn that these study courses and vocational trainings are not only technical but also very versatile. The interviews that were conducted with women are published as a book [48], highlighting the broad spectrum of tasks and activities involved. The gender-sensitive representation of the profession offered by the portraits of women working in the field is designed to focus attention on female role models. Our advice to ISOs is to make use of such gender-sensitive materials, because we know from our research that awareness-raising measures are easier to understand once their benefits for a person's private life become apparent.

Within the Security project, one digital and six analog game-based learning scenarios were developed in German for 9th grade students. Once again, learning scenarios for raising awareness should greatly reduce the complexity of the particular IS topic. The scenarios should use language that is geared to the target group and be presented with appropriate illustrations. Our tests have also shown that these games can provide other age groups with new experience-based insights into IS:

- The scenario *secure school trips* was developed from the analog learning scenario *Security on the go* (e.g., on business trips).
- A new story was constructed (based on a different platform and new personal profile) for the analog/digital scenario *Password hacking*.
- A new background was also created for the analog game *Internet & Apps and the associated risks.*
- Sample emails for the *Phishing learning scenario* were defined that were geared to the target group.
- The analog learning scenario for image utilization and image exploitation rights was redeveloped from scratch and includes two gaming phases.
- The scenario for the simple encryption principle is also more up to date (see chapter 5).
- The developed digital learning scenario "Secure settings for smartphones" can now be used online (see [44]).

Schools can borrow these learning scenarios as a package for their own awareness-raising and training purposes on the project website [46], and ISOs working in education should use this. In addition to the learning scenarios, an entertaining, interactive video on the use of passwords [49] [53] is also available online. The security project is described in the relevant documentation [50].

4.5 Examples from the project *SecAware4school*

In the project "Information security awareness for daily life at school (*SecAware4-school*)", schoolchildren and their caregivers (teachers and parents) are made aware of the topic of information security (IS) [51]. The two-year project is again financed by the Horst Görtz Foundation (HGS) and ends on December 31, 2020. The launch of this project was motivated by the fact that almost all young people and children in Germany have smartphones. The topic of IS should therefore be integrated into the school curriculum at an early stage.

The aim of the SecAware4school project is to raise IS awareness in the target groups in a playful way in order to enable them to carry out their personal risk assessment and handle personal data with care when using Internet services and social media. Teachers should be provided with the necessary materials and instructions to use in the classroom. The aim of the project is to provide pupils with an education in IS that will have a lasting effect.

The digital skills and technical understanding of all those involved are to be enhanced using various measures tailored to the target groups of pupils, teachers, and parents. It is increasingly important for children and adolescents to be able to lead an autonomous life in the digitized world as mature and active people. Parents and teachers, as important adult caregivers for children and adolescents, must also be taken into account in helping young people to develop ways of handling modern technologies and applications confidently and responsibly. In this project, a comprehensive range of support is also being developed and tested for parents and teachers, which enables them to competently assist their children and pupils in acquiring basic digital knowledge on an ongoing basis. The following measures are specifically developed and tested for the target groups:

- The central idea is to train selected pupils from the five pilot schools in the Berlin/Brandenburg region as youth security advisors so that, after the project, they can pass on their knowledge and the skills they have acquired—especially their personal experience in using the game-based learning scenarios—on to other classes with the support of the teachers.

- The focus is thus on three different classes: 6th, 9th, and 11th grades. The respective class level is trained for both their own level and for the levels below. The rationale for this is that young people learn digital skills more easily if they learn with and from each other. All the classes were inspired and guided by the TH Wildau project team, although one school created a new course for 11th grade and was given special support.

- In total, with the five pilot schools and at least two classes in each of the three grades, around 600 young people are involved in the SecAware4school project. It is planned that at least 10 percent can be explicitly trained as security advisors. This is certified through tests from the ICDL module “IT security.”

- Another focus is on imparting basic technical and organizational aspects of information security using experience-based learning scenarios, combined with diversified coaching and mentoring concepts. For the target group of pupils, this does not only mean that these learning scenarios need to be tailored to the concrete everyday situations and language of the children and young people. Rather, for a jointly defined topic, the learning scenarios are developed in a modular way at *three different levels of difficulty* to cater to the three classes.

- Events and (creative) workshops for the three different target classes not only dealt with information but also addressed particular needs and questions, taking these into account in the development of the new learning scenarios. Ultimately, at the end of the project, there will be ten specific analog or digital learning scenarios, each with three different levels of difficulty. The games are offered in German. We are developing the *thirty-six specific experience-oriented learning scenarios* in the SecAware4school project in the following categories:
  - Information security: Rapid guessing (analog)
  - Digital social: Rules of conduct on the Internet (analog)
  - Security surfer: Hazards and protective measures (analog)
  - Online behavior (analog)
  - Fake or real? (analog at six levels)
  - Security duel (analog)
  - Storytelling in information security (analog and digital)
  - Hacker terminal (digital)
  - Rights to photos (digital)
  - Data espionage: Secure room (digital).

These learning scenarios are comprehensively described in the project documentation [52], and the materials will be available for download on the project website in December 2020 [51]. In addition to the learning scenarios, this project provides an entertaining interactive video on the use of passwords in English [53] and is available online as part of the research team’s collection of digital scenarios [44]. In line with the train-the-trainer concept, the material for an advanced training in the ICDL module “IT Security” was given to a selection of teachers in the pilot schools for free, providing them with additional knowledge. This will facilitate and support the preparation of their pupils for the ICDL test. The project also made it possible for five teachers selected by the pilot schools to complete the extensive training and certification as an ISO free of charge (see fig. 91).

4.6 Learning scenarios *Risk Management* and *Social Engineering for SMEs* in the manufacturing sector (DIZ project)

TH Wildau was commissioned by the Research Center for Information Technology (FZI) in Karlsruhe, Germany, to develop two analog learning scenarios (serious games) for the manufacturing industry. The cooperation partners are the "Mittelstand 4.0 - Competence Center Stuttgart" within the Digitization Center (DIZ) in Stuttgart and the participants of the nationwide "IT Security Working Group." A scenario is to be designed specifically for security risk management for executives. The second scenario will deal intensively with the complex topic of social engineering. The scenarios are supplemented by additional information and digital extras (quizzes and tests). The project results will be made available for DIZ events with SMEs on the subject of IT security. This has brought us full circle to the original research projects we carried out on operational awareness in companies.

This one-year DIZ project started on April 1, 2020. Its results are intended to raise awareness among managers and SMEs in general within the manufacturing sector. The project results will be announced in 2021 via the project website [54] as well as via the FZI, the DIZ, and the IT Security Working Group and made available to companies and to a broad cross section of the public.

After the planned creative workshops in April and June 2020 had to be canceled in analog form due to the coronavirus pandemic, two online surveys were carried out by TH Wildau to specify the content and game dynamics to be developed. A report on the development of these two learning scenarios in the lab at TH Wildau (see fig. 91) will be presented in scientific publications and at conferences, and the scenarios will be tested in training courses with SMEs.

Fig. 91 ISO certification training and the development of learning scenarios for IS at TH Wildau.

4.7 Examples from student projects at TH Wildau

Since the elective course “IS awareness raising in companies” was established in summer semester 2017, the game-based learning scenarios have been tested with very good success in different courses and subjects. We also encouraged students to develop a learning scenario as an exam assignment. Depending on the degree program, subject, and topic, these student projects gave rise to interesting ideas with varying levels of maturity. What they all have in common is that the student project teams are able to determine the focus of the topic, reduce its complexity, precisely define the goal, develop the design, and take the “gameplay” into account, allowing them to test the learning scenario, improve it, and ultimately produce everything on a professional level. TH Wildau offers its own diverse range of professional production options. As an additional benefit, the process helps foster team spirit (see fig. 92).

In contrast to the classic format of lecture and practice, the exchange between all participants and the students’ presentations of their own prototypes provide deeper insights into security-relevant questions and the learning process itself. In addition, secondary topics such as didactic questions, project management aspects, and agile development methods are all involved in implementing the students’ projects. Students and lecturers all benefit from the active development of concrete learning scenarios. Ultimately, the entire course structure is transformed: the students become more active, and the lecturer supports them through moderation and coaching.

We continue using student-designed awareness-raising learning scenarios of this kind for other students in subsequent semesters. Our experience both with our own and with student learning scenarios is that three rounds of improvements are necessary before a scenario actually fulfills its potential for raising awareness. In chapter 5, we show examples of some student game-based learning scenarios.

Fig. 92 Promotion of team spirit through experience-oriented learning scenarios for IS.

Please test yourselves with the following questions and comments for chapter 4:

- Can you name the three basic values of information security and give examples in your institution that can endanger them?

- Can you identify the other protection goals of information security for your institution and explain to your colleagues the potential dangers?

- Complete the following sentence: “Managers and employees must be trained in information security because …”

- An awareness-raising and training program is part of the security concept of the institution in line with IT-Grundschutz. Who is responsible for implementation and review in the institution?

- According to research findings, what factors have a major impact on people’s information security awareness and behavior?

- Complete the following sentence: “Experience-oriented learning scenarios are part of an awareness-raising and training concept for information security because …”

Space for your own comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

5. Specific focuses of information security: Technical and Organizational Measures (TOM) geared to ISOs

5.1 Infrastructure for employees: entry – admission – access

An institution has a diverse infrastructure. The infrastructure module (INF) in the BSI *IT-Grundschutz Compendium* [55] consists of the following ten modules. In this chapter, we focus on five of these elements and look at the threats they pose (see table 4):

- INF.1 Building (general)
- INF.2 Data center and server room
- INF.3 Electrical cabling
- INF.4 IT cabling
- INF.5 Room and unit for technical infrastructure
- INF.6 Data carrier archive
- INF.7 Office workstation
- INF.8 Home workstation
- INF.9 Mobile workstation
- INF.10 Meeting, event, and training room

We supplement this overview by taking into account the module *ORP.4 Identity and authorization management* from the BSI *IT-Grundschutz Compendium* [56].

1	**INF.1 Building**	**INF.7 Office WS**	**INF.8 Home WS**	**INF.9 Mobile WS**	**INF.10 Meeting, event, and training room**	**ORP.4 Identity & authorization**
2	Unauthorized entry			Lack of awareness; carelessness		Rights for entry, admission, and access
3	Fire		Lack of or inadequate regulations			Missing or inadequate processes
4	Lightning	Handling by cleaning staff, external personnel, or visitors, and the hazards they pose		Changing operational environment	Hazards posed by visitors	Central deactivation option
5	Water	Manipulation or destruction of IT, equipment, information, and software			Incompatibility between external and in-house IT	
6	Natural hazards and disasters	Theft				
7	Environmental threats	Inappropriate cabling		Delays caused by limited availability	Inappropriate cabling	
8	Violation of laws or regulations	Vandalism	Insecure transport of files and data storage media			
9	Inadequate fire barriers		Unsuitable disposal of data storage media and documents			
10	Power failure	Impairment (of IT use) caused by unfavorable working conditions		Loss of confidentiality of sensitive information		

Tab. 4 Author's summary of the risk situation from selected IT-Grundschutz modules for the "Infrastructure" (INF) of an institution (building, office workstation, home workstation, mobile workstation, meeting and training rooms) and for "Organization & Personnel" (ORP 4: Identity and authorization management).

The module *INF.1 Building (general)* [55] provides a description of the requirements for securing a building from an IS perspective. Buildings are the physical framework for carrying out business processes. They include, among other things, the workplaces/workstations, the processed data, the supporting IT, and utilities such as heating and cooling. In most cases, people outside of the institution also enter the building—e.g., customers, members of the public, suppliers, and business partners—which may pose threats, as shown in the IT-Grundschutz module *INF.10 Meeting, event, and training room* (see table 4). Unauthorized persons should not be allowed to enter sensitive areas of the institution. The term *entry* thus means the right to enter a building or a room. Table 4 shows that, according to IT-Grundschutz, the risks posed by "unauthorized entry" may apply not only to the building but also to the *INF.7 Office workstation* and to the *INF.8 Home workstation* module.

Moreover, the specific threats and vulnerabilities that determine the building's level of risk, as set out in IT-Grundschutz module *INF.1*, are fire, lightning, water, natural hazards and disasters, environmental threats, violation of laws or regulations, inadequate fire barriers, and failure of the power supply (see table 4). For all rooms in the building, the risk of expensive IT systems, mobile devices, and other equipment or data being stolen must also be considered if security measures such as locking and surveillance are not implemented. The IT-Grundschutz defines the possibilities of IT, equipment, data, and software being manipulated or destroyed: this applies to all workstations, be they fixed, home-based, or mobile. Cleaning staff, external personnel, and visitors are of particular importance for rooms, although this does not necessarily involve vandalism but can also include the risk of unintentional damage. A breach of confidentiality through the loss of sensitive information can also lead to data protection problems and have negative internal or external repercussions. Moreover, it also pertains to other damage scenarios according to BSI Standard 200-2. Therefore, regulations for the home or mobile workplace, and for meeting and training rooms must be defined and observed. For example, internal information such as documents, flipchart notes, and technical equipment for presentations must be stored securely, and files, documents, and data storage media must be transported and disposed of safely. In addition, in the meeting, event, and training rooms, possible incompatibilities between third-party IT and the institutional IT must be taken into account. Inappropriate cabling in the office work space should also be avoided as people may trip over this (see table 4).

While the impairment of IT use due to adverse working conditions is of particular importance for workstations in the office and at home, the following specifics are mentioned for the module *INF.9 Mobile workstation* (see table 4):

- lack of security awareness; carelessness
- damage due to changing operational environments
- delays caused by limited availability.

The IT-Grundschutz module *ORP.4 Identity and authorization management* [56] offers a description, geared to the infrastructure, of the risk situations relating to organization and personnel:

- inappropriate entry, admission, and access rights
- lack of or inadequate processes in identity and authorization management
- lack of central deactivation options for user access (see table 4, right column).

An institution should assign individual permissions enabling entry, admission, and access centrally and not on an ad hoc basis. On the other hand, this process should not be unnecessarily complicated. The balancing act turns on the fact that a lack of particular authorizations can be an impediment to day-to-day work, while unnecessary authorizations can lead to a security risk. Where processes in the area of organization and personnel are lacking or inadequate, this corresponds to deficiencies in the infrastructural policies (see table 4).

The *admission* privilege allows a person to use certain IT systems, system components, networks, or computers based on their function and tasks, which requires a login with a username and password. If passwords are used for authentication, the composition of the password should be specified to stipulate, for example, a password length of 12 characters, a certain degree of complexity using upper- and lower-case letters, digits, and special characters, and renewal of the password, say, after one year. These password requirements can also be technically enforced. To avoid the need to write down complicated passwords, the institution needs to take a diplomatic approach and provide support, while also raising the awareness of all employees. This represents a big challenge for ISOs.

Access privileges allow a person to use IT applications (i.e., software) or data based on their function and the range of tasks they need to perform. The use itself must also be specified: e.g., read, write, or execute. Groups and group privileges are often defined in practice in order to simplify administration. Any changes in personnel and individual responsibilities should be noted. Particular attention is required in the event of dismissals or resignations, especially in the case of employee groups like administrators who have almost unrestricted privileges. Special situations must also be monitored, such as with interns working in every department for a while who may end up with a wide range of access rights.

Up-to-date documentation is important. This also requires appropriate logging. In this context, *appropriate* means that the logs can be used to reconstruct the causes of any possible damage that may occur, while observing data protection and employee participation rights.

Table 5 below summarizes the persons responsible for the IT-Grundschutz modules selected in table 4. We have made two additions: firstly, we have explicitly included fire protection as one of the responsibilities covered by module *INF.1 Building*, because under the requirement for basic protection *INF.1.A3 Compliance with fire protection regulations (B)*, it says, "There MUST be a fire protection officer (FPO) or a person entrusted with this area of responsibility who is also appropriately trained" [55]. Secondly, we have added the ISO to module *INF.10 Meeting, event, and training room*, because ISOs have to include such rooms when devising the security concept for an institution. The primary responsibility of an ISO for the *INF.1 Building* module is the drafting of the IS concept, which includes the building (see table 6).

	INF.1 Building	INF.7 Office	INF.8 At home	INF.9 Mobile	INF.10 Meeting, event, and training room	ORP.4 Identity & authorization
A	On-site facility engineer	**ISO**	Employees	**ISO**	Organizational management	**ISO**
B	Construction management Construction company **ISO** Internal service Institution management Organizational management Employees Planning department **FPO**	Facility management IT management Employees Managers	On-site facility engineer **ISO**	IT operation IT management Employees HR department	On-site facility engineer IT operation IT management Employees **ISO**	Users IT operation

Tab. 5 Authors' summary of responsibilities based on the IT-Grundschutz Compendium [55] [56] with certain additions made. A = main responsibility, B = further responsibilities.

Requirement identifier	Infrastructure requirement for a building
INF.1.A1	Planning of building safeguards [planner] (B)
INF.1.A2	Adapted distribution of the power circuits (B)
INF.1.A3	Compliance with fire-protection regulations (B)
INF.1.A4	Fire detection in buildings [planner] (B)
INF.1.A5	Hand fire extinguisher (B)
INF.1.A6	Closed windows and doors [employees] (B)
INF.1.A7	Entry regulation and control [head of organization] (B)
INF.1.A8	Smoking ban (B)
INF.1.A9	**Security concept for use of the building [planner, ISO] (S)**
INF.1.A10	Compliance with relevant standards / regulations [construction company, construction manager] (S)
INF.1.A11	Locked doors [employee] (S)
INF.1.A12	Key management (S)
INF.1.A13	Regulations for entry to distribution boards (S)
INF.1.A14	Lightning protection devices (S)
INF.1.A15	Site plans of feed lines (S)
INF.1.A16	Shielding of information about parts of the building that need to be kept secure (S)
INF.1.A17	Structural smoke protection [planner] (S)
INF.1.A18	Fire protection inspections (S)
INF.1.A19	Information provided in good time by fire protection officer (S)
INF.1.A20	Alert plan and fire protection drills (S)

Tab. 6 Authors' overview of the infrastructure building requirements as per the IT-Grundschutz module INF.1 [55]. The security concept (standard protection), which is central to ISOs, is shown in bold.

Requirement identifier	Requirements for organization and staff
ORP.4.A1	Planning of building safeguards [planner] (B)
ORP.4.A2	Procedure for setting up, changing, and withdrawing authorizations [IT operations] (B)
ORP.4.A3	Documentation of user IDs and rights [IT operations] (B)
ORP.4.A4	Distribution of tasks and separation of functions [IT operations] (B)
ORP.4.A5	Allocation of entry authorizations [IT operations] (B)
ORP.4.A6	Allocation of admission authorizations [IT operations] (B)
ORP.4.A7	Allocation of access privileges [IT operations] (B)
ORP.4.A8	Administration of password use [users, IT operations] (B)
ORP.4.A9	Identification and authentication [IT operations] (B)
ORP.4.**A22**	Administration of password quality [IT operations] (B)
ORP.4.**A23**	Administration of password-processing applications and IT systems [IT operations] (B)
ORP.4.A10	Protection of user IDs with extensive authorizations [IT operations] (S)
ORP.4.A11	Resetting passwords [IT operations] (S)
ORP.4.A12	Development of an authentication concept for IT systems/applications [IT operations] (S)
ORP.4.A13	Appropriate selection of authentication mechanisms [IT operations] (S)
ORP.4.A14	Control of the effectiveness of user separation on the IT system/application [IT operations] (S)
ORP.4.A15	Procedure and conception of the processes for identity and authorization management [IT operations] (S)
ORP.4.A16	Guidelines for admission and access control [IT operations] (S)
ORP.4.A17	Appropriate selection of identity and authorization management systems [IT operations] (S)
ORP.4.A18	Use of a central authentication service [IT operations] (S)
ORP.4.A19	Briefing of all employees in the use of authentication procedures and mechanisms [users, IT operations] (S)
ORP.4.A20	Contingency planning for the identity and authorization management system [IT operations] (H)
ORP.4.A21	Multi-factor authentication [IT operations] (H)

Tab. 7 Authors' overview of the requirements for identity and authorization concepts as per the IT-Grundschutz module ORP.4 [56]. (B) identifies the requirements for basic protection, (S) the additional requirements for standard protection, and (H) the additional requirements for a higher level of protection. The ISOs have "fundamental responsibility" for this module. It should be noted that requirements 22 and 23 already represent basic requirements. Requirements 20 and 21, on the other hand, relate to an organization's increased protection needs.

Table 6 summarizes the requirements resulting from IT-Grundschutz from the risk situations of the selected module *INF.1 Building* (see table 4) as an overview. For ISOs, the requirement *INF.1.A9 Security concept for use of the building [planner, ISO] (S)* is key, because, together with the "planner," the staff involved are in essence responsible for the devising the organization's security concept. This requirement is part of its standard protection (S) and therefore goes beyond basic protection (B).

Table 7 shows the summary of the requirements for the module *ORP.4 Identity and authorization management*, for which the ISOs have "fundamental responsibility" according to IT-Grundschutz [56]. The basic requirements are marked in the table with a (B), while an (S) indicates the additional requirements for standard protection and an (H) applies to the additional requirements for a higher level of protection. However, we do not deal with the last category here. The IS requirements for workplaces and rooms based on IT-Grundschutz modules INF.7 to INF.10 [55] are grouped together in table 8. ISOs are fundamentally responsible for all requirements of the IT-Grundschutz modules *INF.7 Office workstation (WS)* and *INF.9 Mobile WS*, while this responsibility shifts to the individual employees in the case of module *INF.8 Home WS*. In this respect, ISOs only have one additional responsibility, including as a central contact person.

INF.7 Office WS	INF.8 Home WS	INF.9 Mobile WS	INF.10 Meeting & training rooms
INF.7.A1 **Suitable selection and use of an office space [employees, supervisors] (B)**	INF.8.A1 Securing of official documents at the home workstation (B)	**INF.9.A1** **Appropriate selection and use of mobile workstations [IT operation] (B)**	INF.10.A1 Safe use of meeting, event, and training rooms [facility engineer, IT manager] (B)
	INF.8.A2 Transport of work material to the home workstation [building services] (B)	**INF.9.A2** **Regulations for mobile workstations [HR department] (B)**	INF.10.A8 Creation of a certificate verifying room usage (S)
INF.7.A2 **Closed windows and locked doors [employees] (B)**			INF.10.A3 Closed windows and locked doors [employees] (B)
INF.7.A4 **Entry regulations and access control (S)**	INF.8.A3 Protection against unauthorized entry at the home workstation (B)	**INF.9.A3** **Entry and access protection [HR department] (B)**	INF.10.A2 Supervision of visitors [employees] (B)
		INF.9.A4 **Working with external IT systems [head of IT] (B)**	INF.10.A6 Establishing secure network access [head of IT] (S)
		INF.9.A5 **Prompt notification of loss [employees] (S)**	INF.10.A4 Planning of meeting, event, and training rooms (S)
INF.7.A5 **Ergonomic workstation [chief facility engineer] (S)**	INF.8.A4 Suitable furnishing of the home workstation (S)	**INF.9.A7** **Legal framework for mobile working [HR] (S)**	INF.10.A7 Secure configuration of training and presentation computers [head of IT] (S)
INF.7.A6 **Clear workstation [employees] (S)**	INF.8.A5 Disposal of confidential information in the home workstation (S)	**INF.9.A6** **Disposal of confidential information [employees] (S)**	
INF.7.A7 **Suitable storage of official documents and data carriers [employee, head of building services] (S)**		**INF.9.A8** **Security guidelines for mobile workstations [head of IT] (S)**	
		INF.9.A9 **Encryption of portable IT systems and data carriers [IT operations] (S)**	
INF.7.A3 **Loose cabling (S)**			INF.10.A5 Loose cabling (S)

Tab. 8 Authors' overview of the requirements for the IS of the workstations and rooms as per the IT-Grundschutz modules INF.7 to INF.10 [55]. (B) identifies an organization's basic requirements, while (S) indicates the additional requirements for standard protection. The ISOs' basic area of responsibility according to the IT-Grundschutz Compendium is shown in bold.

IT-Grundschutz does not designate any responsibility to ISOs for meeting and training rooms. However, the need for these rooms to be included in the organization's security concept is evidence of the supporting role played by ISOs.

Implementation and training exercises to raise awareness

The compiled list of IT-Grundschutz requirements indicates to the ISOs that there is a considerable need for acceptance and therefore a need to raise awareness. We would like to encourage ISOs to *actively* include entry, admission, and access rights in their awareness-raising measures. ISOs can carry out awareness-raising measures themselves, sometimes using simple means. In all awareness-raising measures, it is important that the examples and materials used actually correspond to working life in the institution. This means that our following exercise instructions should be adapted to the specific organization with its specific documents.

The first exercise that we present in this chapter relates to entering a room. It's a remarkably simple and quick exercise, highlighting the importance of the sensitive data, information, and items that should be locked away when you leave the office. It is called *Clear Desk* (see fig. 93). The idea is part of the Security Arena and comes from the company known_sense [39]. In the exercise, the participants are asked to categorize a collection of different materials and assign them to particular areas ("locked" = red area, "leave" = green area). Participants recognize very quickly which information and objects they should not leave lying around in the office—this is evidently not problematic at the theoretical level. What is important about this exercise is the subsequent exchange about the real situation in the organization or institution, and experience has shown that things often look quite different in practice.

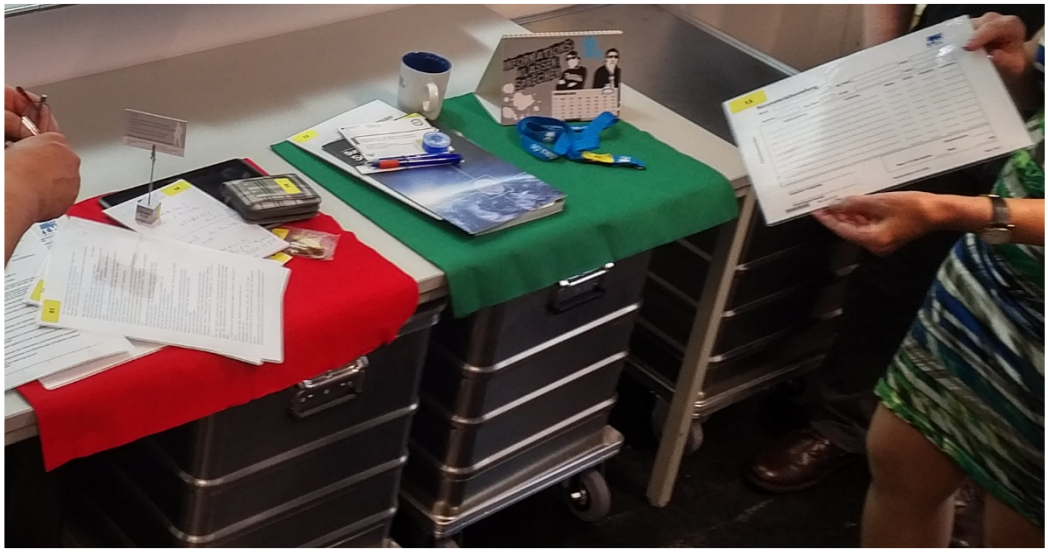


Fig. 93 Exercise "Clear Desk" in the TH Wildau version. The idea of this game-based analog learning scenario comes from the Security Arena and is licensed by known_sense [39].

The research group is currently developing a similar digital learning scenario. This electronic version, called *Secure Room*, should be available in German at the end of 2020 and be generally accessible on the website [44].

In connection with the protection of valuables, this exercise looks at methods like Radio Frequency Identification (RFID) and Near Field Communication (NFC), which were developed for the automatic identification of objects via radio. Depending on the frequency range and design, data can be transmitted over distances between 0 and approx. 7 meters from an RFID chip to a reader—with NFC, this works in both directions. In principle, such systems consist of a transponder and a reader (see [57]). The transponder is either attached to an object or integrated into an object. The latter is the case with chip cards, where the chip and the antenna are hidden inside the card and cannot always be seen. In the case of cash cards, the radio wave symbol (fig. 94) indicates this possibility of transmission, with a short transmission distance of a few tens of centimeters. Nonetheless, attackers equipped with an appropriate smartphone as a mobile reading device can try to scan the wallet or bag and cull data. RFID or NFC blockers in card format can prevent this information from being read.

Fig. 94 Radio wave transmission symbol.

Another exercise, which fits in with the focus of this chapter, was developed by a team of students from the Administrative Informatics course (VIBB-18) as part of the *Smart Home* assignment in the first semester (see fig. 95).

Fig. 95 "Smart Home (IoT)"–analog game-based learning scenario in three phases. Developed in the 1st semester as part of the Information Security and Awareness (ISA) component of the Administrative Informatics course (VIBB-18) at TH Wildau. Concept, design, and production by Denny Ratter, Alexander Schröder, Björn Thiel, Jannik Walter, Tobias Walter, and Paul Zeskowski, January 2019 [58].

The game-based learning scenario is structured in three phases. Phase 1: An office worker (top-right corner in fig. 95) controls his smart home remotely from his work area. First of all, the participants have to position the IoT devices in the right place on the smart-home poster (blue-and-white cards with symbols). Phase 2: Next, the technical properties of the IoT devices must be assigned (orange cards). Phase 3: Finally, possible dangers are identified and assigned (green cards). The scenario provides a good basis for discussion.

The mobile workstation, already dealt with in tables 4, 5, and 8 from the point of view of IT-Grundschutz, is an increasing challenge for all institutions. The employees work in a mobile setting, both within the organization and at a variety of external workstations. The module *INF.9 Mobile workstation* could also be applicable for any rooms that are commonly used as a mobile workplace [55]. According to IT-Grundschutz, the primary focus of this module is on mapping the organizational, technical, and personal requirements for work that is completely or partially mobile. ISOs, however, have to take into account further modules in order to secure IT systems, data carriers, or documents that are used during mobile work. The *IT-Grundschutz Compendium* refers to the following modules, which should be considered relevant: *SYS.3.1 Laptops*, *SYS.3.2 General smartphones and tablets*, *SYS.4.5 Removable storage*, *NET.3.3 VPN*, and *SYS.2.1 General client* [55]. Teleworking stations are also described separately in the module *OPS.1.2.4 Teleworking*. A mobile workstation is necessary for business trips, be it domestically or abroad. For this purpose, there is the special module *CON.7 Information security on trips abroad* [59] with corresponding implementation instructions (still in version 2019) [42]. The CON area of the *IT-Grundschutz Compendium* stands for *Concepts and Procedures*. There are a range of risk situations defined in *CON.7 Information security on foreign trips* [59]. These include eavesdropping and spying on information, industrial espionage, and the disclosure and misuse of information that should be protected (electronic and physical); false identity or information from an unreliable source; lack of security awareness, carelessness in handling information and unnoticed access to mobile devices as well as theft or loss of devices, data carriers, and documents; violation of local laws or regulations as well as coercion, blackmail, kidnapping, and corruption. Further details can be found on the webpage of the information portal Initiative Wirtschaftsschutz [60].

According to module CON.7, ISOs have overall responsibility for IS on foreign trips made by employees on behalf of the institution or organization, while the travelers themselves, as well as the IT operations and HR departments of the institution, are responsible for security. The information, publications, and travel warnings issued by the Federal Foreign Office should also be observed. Business trips in Germany and, more particularly, abroad can contain such a wide range of threats that it is imperative to raise employees' awareness. Depending on the institution, more in-depth training measures must also be provided. ISOs must initiate this (see fig. 1).

Fig. 96 (above) Use of the analog learning scenario "Security on the Go" with fourteen stations, based on possible incidents during business trips. The game-based analog learning scenario is licensed as part of the Security Arena from known_sense [39].

Fig. 97 (right) Redeveloped version of the analog serious game "Security & Safe on Class Trip" (in German) with 6 stations in the "Security" project. The learning station is freely available to schools and can be borrowed from the Security Project website [46].

To raise awareness, we can recommend "Security on the Go," one of the learning stations from the Security Arena produced by the company known_sense [39] (see fig. 96), in which participants can exchange information on fourteen possible incidents in two phases: in the first phase, the idea is to discover the fourteen incidents on the basis of situation descriptions, while in the second phase simple security measures are to be assigned. The use of this experience-oriented learning scenario has so far been given a very positive rating by all course participants. The Research Group Scholl has further developed this analog game idea for schools (see fig. 97) in order to raise awareness of safety on school trips (see [50]). Schools can borrow the learning scenario free of charge from the *Security* project website, simply by paying the postage [46]. ISOs in schools can therefore carry out this kind of awareness raising at very low cost.

Game-based sensitization aims to increase people's awareness in the long term. In connection with the above risk situations identified in the IT-Grundschutz module *CON.7*, an analog game development by students of the Administrative Informatics course VIBB-19 entitled *Working in public environments* [61] can be used as another example that has been extensively tested (see fig. 98). The starting point for this learning scenario is that pressure and stress, for example, can lead to negligence and a lack of attention. In such situations, employees do not have a proper sense of IS-related risk. Therefore, players should be able to easily put themselves in everyday scenarios and analyze the situation quickly. In addition to having fun, competition between small groups was built into the game—this is often used successfully in "gamification" and involves team building based on the goal of winning together as a group, working against the clock with a bell, and collecting points for evaluation. The sources of danger must be recognized quickly and countermeasures must be identified immediately in order to secure the points.

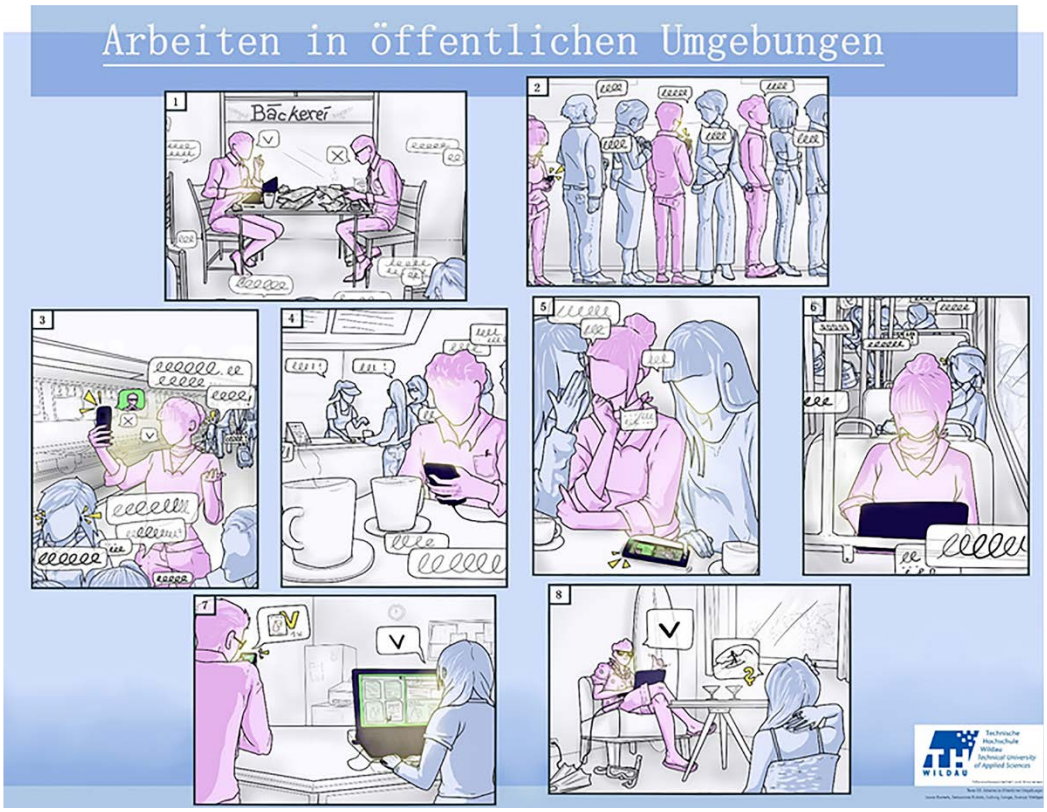


Fig. 98 *"Working in public environments"–analog game-based learning scenario in eight scenes. Developed in the 1st semester in the Information Security and Awareness (ISA) component of the Administrative Informatics course (VIBB-19) at TH Wildau. Conception, design, and production by the group Svenja Weltjen, Sebastian Kubitz, Jonas Bartels, and Ludwig Lange, January 2020 [61].*

The eight scenes of the learning station *Working in public environments* (fig. 98), which are shown successively in the exercise, were drawn by Svenja Weltjen on her own initiative and contain the following situations [61]:

- Scene 1: Our two employees go to a bakery during a breakfast break. There they continue to work together on relevant documents.
- Scene 2: Three of our employees go to the large canteen during their lunch break. Although this is on the company premises, it is also accessible to external parties and, thanks to the low prices, is very popular.
- Scene 3: Our employee is standing at the station and waiting for her train. In order to make the best use of her time, she makes a call about her project—there are still many details to clarify.
- Scene 4: Our employee missed his train and because he has a bad conscience about being late for work, he is processing a few important documents on his cell phone in a burger joint next door.
- Scene 5: Our employee meets two new friends during her lunch break and is happy to have a real break because her colleague is constantly bugging her about the deadlines for upcoming projects.
- Scene 6: Our employee's car suddenly won't start, and so she takes public transport home in the evening and continues to work on the bus.

- Scene 7: The in-house printer has “flipped out again” and today of all days there are many printouts needed for an important meeting. Fortunately, our employee knows a good copy shop next door.
- Scene 8: Finally, the project is over and the long-awaited vacation with loved ones in Hawaii can start. But no sooner has our employee arrived than he receives a Skype call from a colleague saying that something important still needs to be worked on. Our employee is known for his speed and can do everything in the hotel room within an hour.

Another increasingly common form of attack that requires additional awareness-raising measures as part of the IS focus on entry, admission, and access rights is social engineering (SE). The elementary threat 0.42 of IT-Grundschutz deals with this special form of attack in more detail [62]. The term is often still unknown to many respondents. SE means personal interactions involving manipulation by unauthorized persons with the aim of gaining access to information or IT systems under false pretenses. Social engineers therefore first target employees as individuals in order to access an organization’s important information or sensitive data. According to the study “Bluff me if U can” [63], communication in the digital world and people as social beings play a decisive role. SE attacks therefore take place at people’s “social gateways,” which include curiosity, the desire for acknowledgement, and a willingness to help [63] (see fig. 99). Awareness raising should lead to participants reflecting more consciously on their own communication behavior and their personal characteristics (gateways). The Security Arena of the company known_sense [39] contains an SE learning station focused on six social gateways.

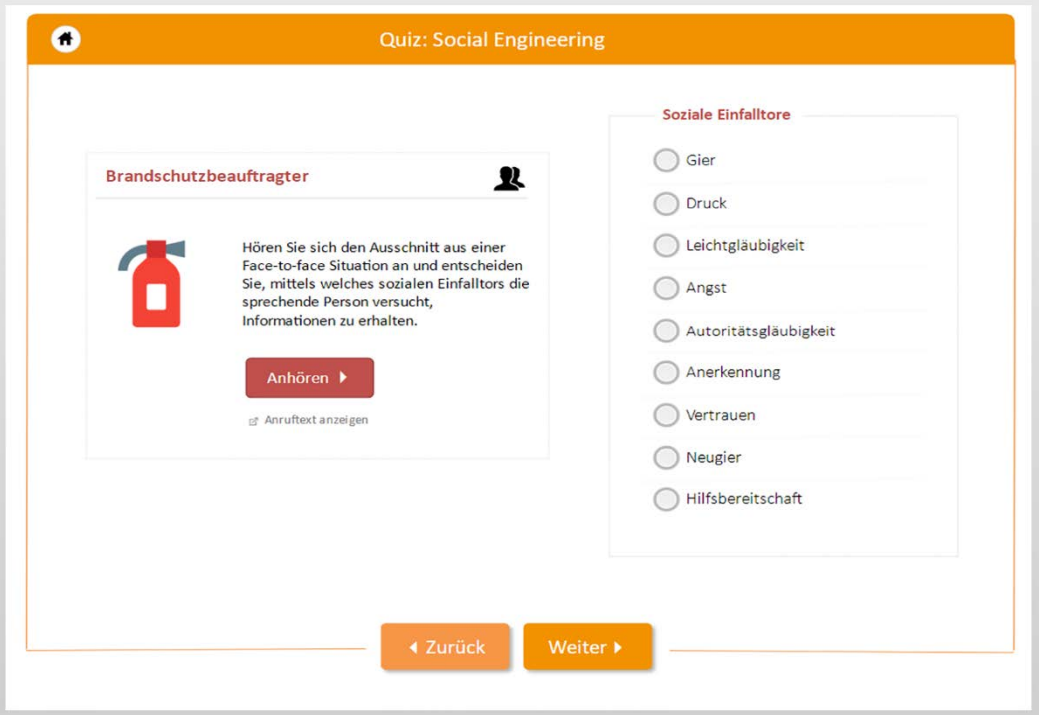


Fig. 99 Digital game-based learning scenario “Social Engineering” devised at TH Wildau and designed to promote self-reflection (in German) [64].

As part of the SecAware4job project, the research group developed a digital version with a total of nine gateways (see fig. 99), which can be freely used to help students raise their own levels of awareness [64]. Listen to the examples and decide which social gateways social engineers use to reach their goal.

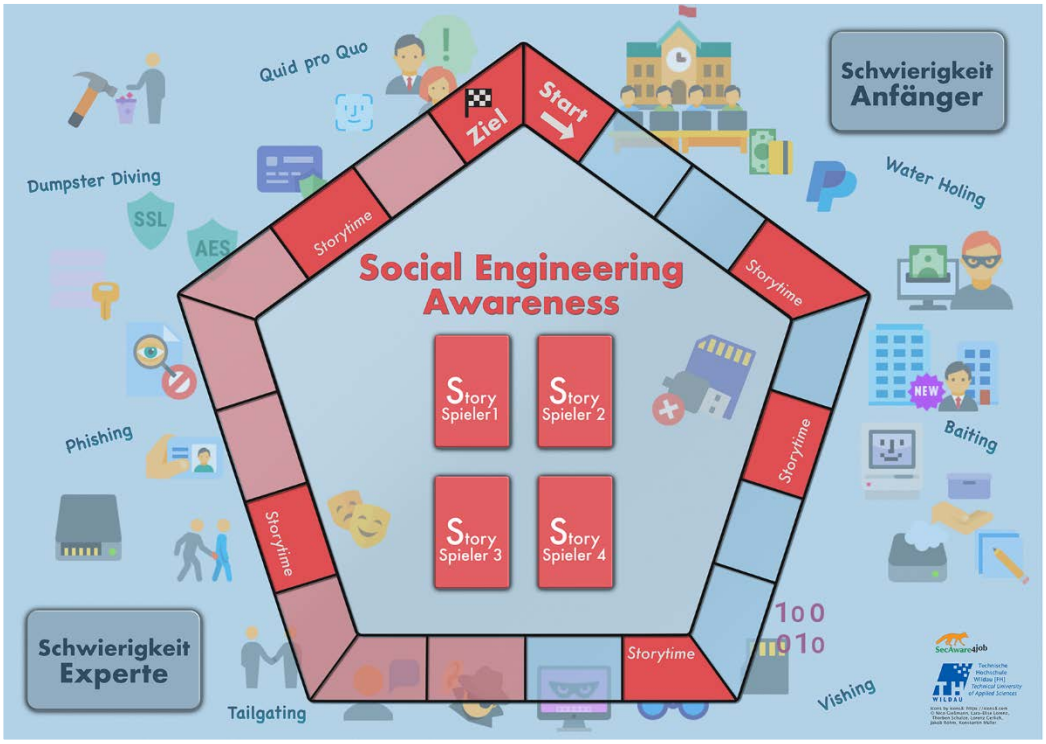


Fig. 100 *"Social Engineering Awareness"—analog game-based learning scenario with two levels of difficulty and four accompanying SE stories. Developed in the 1st semester in the Information Security and Awareness (ISA) component of the Administrative Informatics course (VIBB-18) at TH Wildau. Concept, design, and production by the group Nico Gießmann, Lorenz Gerlich, Konstatin Müller, Lara-Elise Lorenz, and Jakob Röhm, January 2019 [65].*

Fig. 101 *"Social engineering risks"—analog game-based learning scenario in five phases. Developed in the 1st semester in the Information Security and Awareness (ISA) component of the Administrative Informatics course (VIBB-19) at TH Wildau. Concept, design, and production by the group Robert Wernitz, Rocco Krüger, Christoph Zimmermann, and Michel Darkow, January 2020 [66].*

The SE mode of attack was also the topic of analog scenarios developed by two other student project teams. In the first case, a board game was created in 2019 with question cards at two different levels of difficulty, “beginner” and “expert,” as well as four accompanying “SE stories” (fig. 100). In the second case, a matching game was developed in 2020 (fig. 101) in which key risks are assessed.

The long-standing and still lucrative phishing attack must also be spotlighted in connection with the IS focus on entry, admission, and access privileges. It is an artificial word, made up of password and fishing, that refers to criminal offenses ranging from data theft and account withdrawals to attacks on critical infrastructures [67]. The BSI provides extensive information on this under its heading “BSI for citizens,” and presents videos [67] and articles [68] to raise awareness. Particularly in times of crisis, fraudsters and criminals use every opportunity to earn significant amounts of money by exploiting the uncertainty and hopes of many people. Therefore, in 2020, the BSI expressly warns against emails relating to the coronavirus and urges special caution [68]. Fishing for employee passwords gives attackers easy access to the IT systems and applications being used. For this purpose, the FS had developed its own digital learning scenario to help raise awareness in the SecAware4job project (fig. 102), which is freely accessible [69]. In addition to a brief explanation, two tests can be completed. The first self-test is about recognizing phishing emails. In the second self-test, the identifying features of the phishing emails that are presented must be worked out in detail.

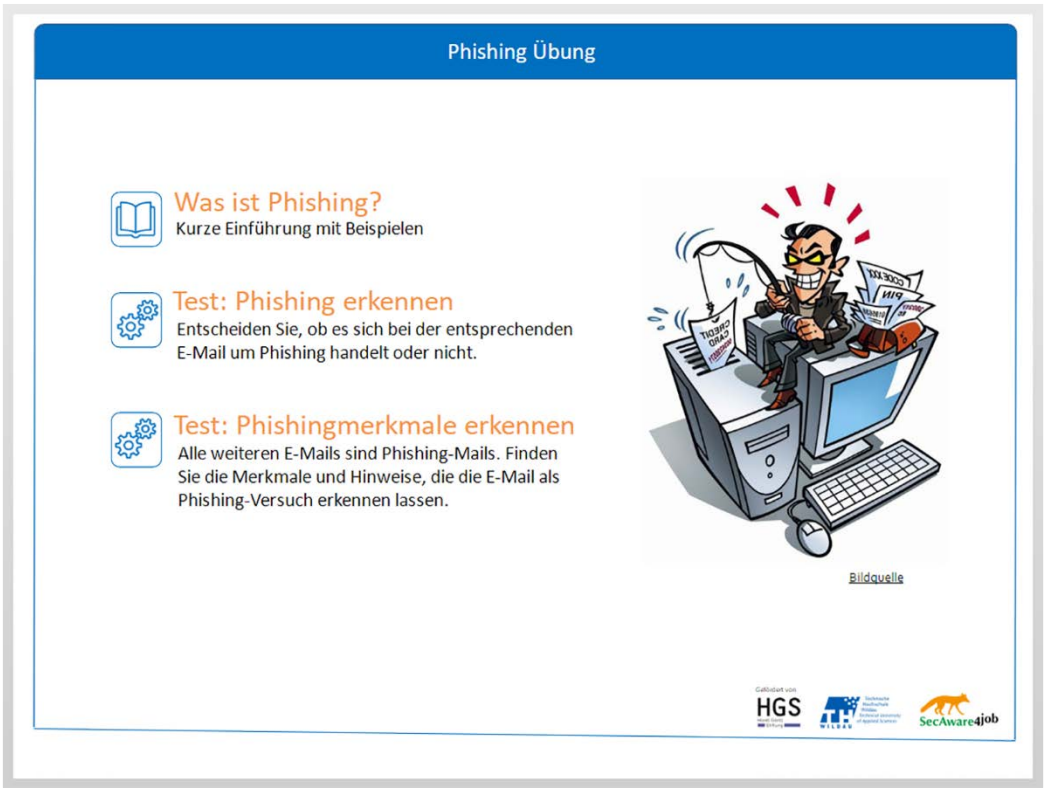


Fig. 102 Digital game-based learning scenario “Phishing” developed by the research team at TH Wildau and designed to promote self-reflection (in German) [69].

The next two awareness exercises also deal with passwords. We know from psychology-based research that putting yourself in the position and mindset of an attacker can be extremely useful and stimulating. In the case of passwords, this means trying to infer their configuration from the information disclosed by a victim. Attackers can prey on the profile data published on social networks if people do not carefully "construct" their passwords. This exercise, which is called Password Hacking, comes from the known_sense Security Arena [39] and was adapted by the research group: firstly, in the SecAware4job [43] project for students at TH Wildau and, secondly, in the Security [46] project for students in the pilot schools (see fig. 103). In our experience, this experience-oriented learning scenario is popular with everyone. The complexity is reduced by simple passwords in order to make the learning scenario playable, but it is precisely through this that sustainable awareness is achieved. You can refer to websites that show how long a computer needs, based on the current state of technology, to find out a password of varying complexity. The evaluation can also be carried out to different degrees, depending on the target group. For example, students can also discuss the so-called hash values that are now used to store passwords in encrypted form.

Fig. 103 *Analog-digital learning scenario "Password Hacking" in the version created by TH Wildau for schools (in German). The idea comes from the Security Arena and is licensed by known_sense [39].*

The next fun exercise we have selected is designed in such a way that an awareness of secure passwords is promoted by guessing terms. It is still being developed by the Research Group Scholl and is called *Terminal Hacker* [70]. This is based on an anagram and a reference to the password. These exercises are supplemented by an interactive video on secure passwords that was produced in German for the *Security* project [49] and in English for the *SecAware4school* project [53] (see fig. 104).

The video is interactive, as the video sequences take a different course depending on the user's selection of possible behavior patterns (see fig. 104).

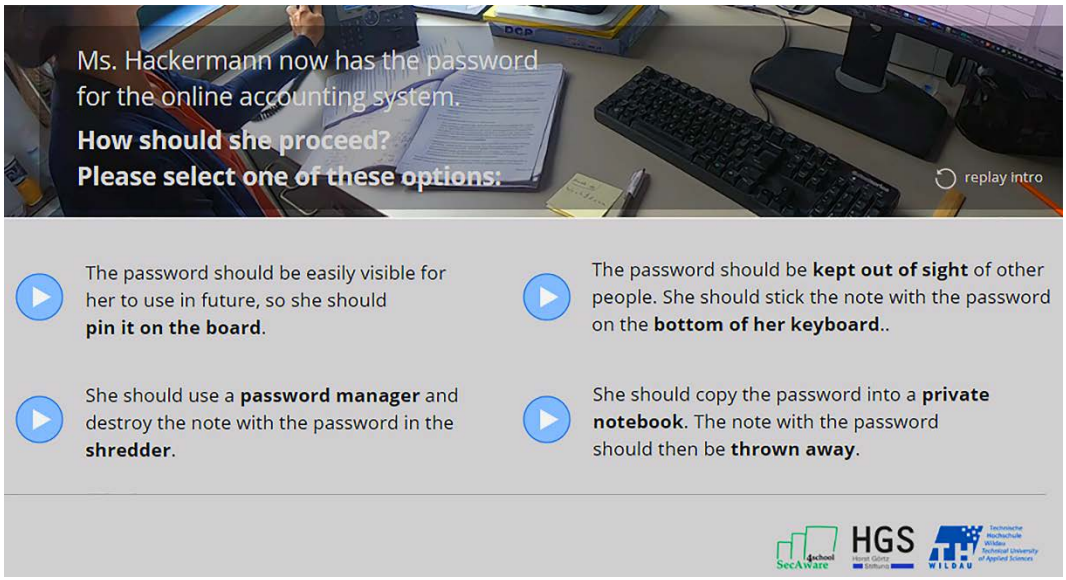


Fig. 104 Interactive training video on secure passwords developed by the Research Group Scholl [49] [71].

Both ISOs and employees must be familiar with the laws, policies, and operational guidelines that apply to their activities. In particular, they should be aware of the criminal offenses set down in the Criminal Code (StGB) to cover computer crime, and to familiarize them with this, an entertaining, freely usable game in digital form was also developed in the *SecAware4job* project (fig. 105). It deals with the following paragraphs of the Criminal Code [72]:

- § 202a StGB: Spying on data and § 202b StGB: Interception of data
- § 202c StGB: Preparing to spy on and intercept data
- § 202d StGB: Data theft
- § 263a StGB: Computer fraud
- § 269 StGB: Falsification of data with evidential value
- § 267 StGB: Forgery of documents
- § 270 StGB: Deception in legal transactions when processing data.

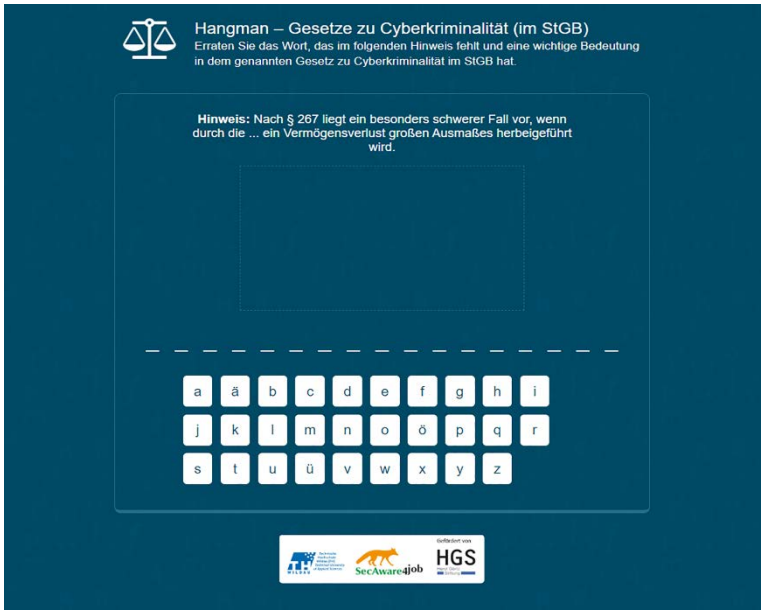


Fig. 105 Digital learning scenario for the StGB law developed by the Research Group Scholl at TH Wildau (in German) [72].

Please test yourself with the following questions and comments on chapter 5.1:

- Can you explain the three terms “entry rights,” “admission rights,” and “access rights,” and how they are differentiated?

- Can you clarify to the management of your institution the risk situations pertaining to office, home, and mobile workstations as well as to meeting and training rooms?

- Can you explain the primary responsibilities of information security officers for the infrastructure modules of the IT-Grundschutz?

- Can you explain to your colleagues the need for appropriate logging?

- Can you explain the risk situations pertaining to business trips abroad according to IT-Grundschutz?

- What specific measures can your organization use to protect itself against social engineering attacks?

- Complete the sentence: “The goals of a game-based awareness-raising measure are …”

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

5.2 Data backup concept and data media

The importance of data security policies and concrete concepts was made clear to the public in 2016, primarily through the many ransomware incidents that took place in Germany, Europe, and worldwide: many institutions were asked to make Bitcoin payments in order to get their foreign-encrypted data back. It was particularly noteworthy that, despite making the payment and receiving the key, victims could not always recover all their data. On the contrary, extensive data loss resulted, with the consequence that the organizations had to ask customers for their data again and thus risked further damage to their image. None of this need have happened if the organization had had a sound data security concept and tested it regularly so that it is clear how much time the IT administration needs to restore the data if necessary. Therefore, this is a crucial issue for ISOs that must be clarified in coordination with the organization's administrators.

A data backup *strategy* is intended to safeguard an organization's operational data inventory using redundant data storage. In order to create a sustainable data backup concept, the ISOs and administrators must therefore do the following:

- Understand and record the requirements of the organization;
- Have a basic understanding of data protection concepts;
- Assess the appropriateness of the concepts;
- Recognize defects and develop suggestions for improvement.

This enables the management of the institution to make competent decisions about the concept that has been developed.

There are a number of general questions relating to a data backup concept:

- What data do I back up?
- When do I save it?
- How often do I back it up?
- What backup procedure do I use?
- What storage media do I use?
- How is the media transported and stored?
- Who is responsible for the technical side?

The following questions focus on the specific requirements for data backup:

- What data and files are modified and how often do they change?
- How high is the data volume in each case?
- How extensive are these changes?
- Is personal data involved?
- Do deletion periods need to be observed? Have retention periods been established?
- What cost considerations apply to data backups?

- Do we know the costs in the event of malfunction? Can we determine this?
- What are the requirements for data availability, confidentiality, and integrity?
- How much effort does it take to reconstruct or recreate the data?
- Are there tests and drills for restoring the backup? How often and how frequently do they take place?

The data backup concept can be found in the IT-Grundschutz in the *CON conception and procedures* area and is dealt with specifically in *CON.3* [73]. The following risk situations are identified there:

- No data backup
- No recovery tests
- Unsuitable storage of the backup media
- Lack of or insufficient documentation
- Disregard of legal regulations
- Insecure cloud providers
- Insufficient storage capacity
- Inadequate data backup concept.

Particular attention should be paid to the following hazards in practice:

- Demagnetization (due to aging or environmental conditions)
- Destruction (by fire, water, or force majeure)
- Accidental deletion or overwriting
- Media errors
- Deliberate destruction.

A data backup concept must be differentiated from *archiving*: archiving is permanent storage, in compliance, for example, with long statutory retention periods. Archiving is not a substitute for data backup! Archiving is dealt with in the IT-Grundschutz module *OPS.1.2.2 Archiving* [74], in connection with *OPS operation*. Using the technical guidelines of the BSI [75], individual aspects can be dealt with in greater depth, such as the deletion and destruction of classified information on data carriers [76].

According to IT-Grundschutz, the ISOs are responsible for checking the data security concepts. The other responsibilities lie with the technical managers, IT operations, and IT management [73]. *CON.3 Data backup concept* [73] formulates the following requirements for basic and standard protection:

- CON.3.A1 Survey of the influencing factors for data backups [persons responsible, IT operations] (B)
- CON.3.A2 Determination of the procedure for data backup [persons responsible, IT operations] (B)
- CON.3.A4 Creation of a minimum data backup concept [IT operation] (B)

- CON.3.A5 Regular data backup [IT operations] (B)
- CON.3.A6 Development of a data backup concept [specialist, IT operations] (S)
- CON.3.A7 Procurement of a suitable data security system [head of IT] (S)
- CON.3.A9 Requirements for online data backup [IT operations, IT manager] (S)
- CON.3.A10 Obligation of employees to back up data (S)
- CON.3.A11 Backup copy of the software used [IT operations] (S)
- CON.3.A12 Suitable storage of the backup data carriers [IT operations] (S).

ISOs should understand the following terms in relation to data backup strategies and criteria and be able to explain the differences between them:

- Full data backup
- Differential data backup
- Incremental data backup
- Virtual full data backup
- Memory image backup
- Backup times and the generation principle
- Data storage media selection criteria.

Fig. 106 outlines the first three backup strategies mentioned. With a full data backup, all data that should be backed up is saved, regardless of whether it has changed since the last data backup (fig. 106, 1st backup). A full data backup thus requires significant storage space. On the other hand, the entire database is available in full at all times.

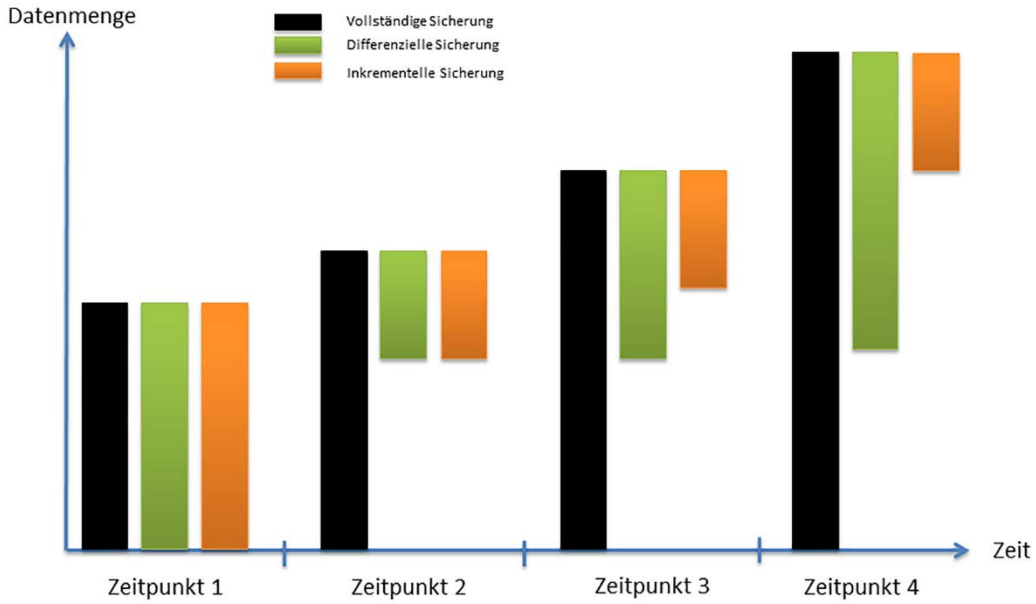


Fig. 106 *Authors' sketch of the data backup strategies* Full data backup *(shown in black),* Incremental data backup *(in orange) and* Differential data backup *(in green). When saving for the first time (*Zeitpunkt *1), all three backups create a full data backup. Differences only arise when the data to be saved has changed (see 2nd, 3rd, and 4th backups [in German:* Zeitpunkt *2, 3, 4]).*

With a *differential data backup*, data is saved that has changed since the last full data backup. In the second backup, as shown in fig. 106, data is stored that has changed as compared to the first backup. For the second and third backups, this data volume increases because the storage is independent of the other differential data backups and only relates to the last full data backup.

In the case of an *incremental data backup*, only the data that has changed since the last backup is saved, regardless of whether it was a full data backup or an incremental backup. Fig. 106 thus shows the same stored data volume at backup 2 as the differential data backup. After that, however, the storage space requirement is less than with differential data backup and far less than with full data backup. Incremental data backup saves storage space and at the same time shortens the time required to back up the data. However, the time required to restore data is greater, since all incremental backups must be included in the last full data backup.

In addition to the three common types of data backups shown, there are two additional techniques to be considered. First, there is the virtual full data backup (fig. 107). Like the full data backup, a complete backup storage is created in which all data is restored. However, in contrast to the full data backup, the productive data is not used. Several backups (differential backups or incremental backups) are used as the source in order to correspond to a complete backup of the collected data at a specific point in time. This type of storage is mostly used for separate storage or, if the time windows are too small, for backing up productive data. Since a new full backup is created here, the resulting chain of incremental backups can also be restarted after creating a virtual full data backup.

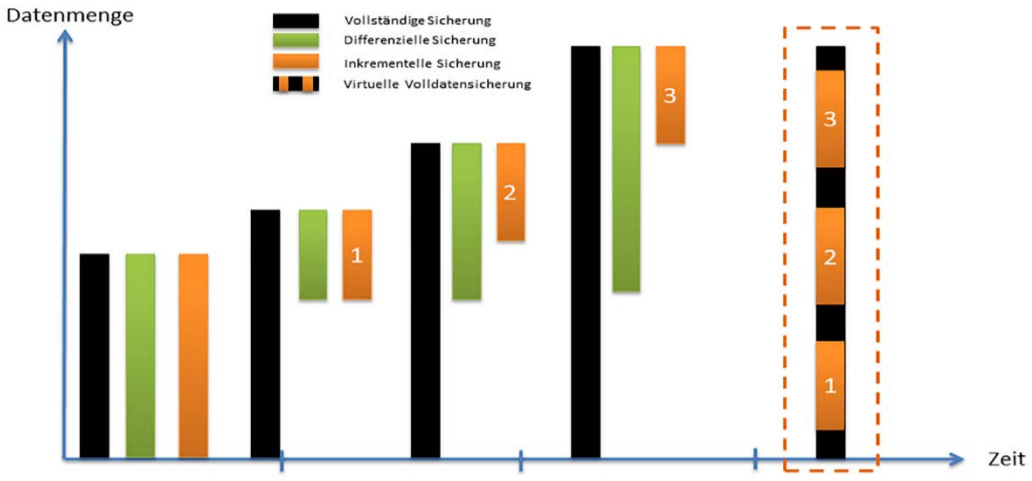


Fig. 107 Author's sketch correlating to fig. 106, supplemented by the virtual full data backup.

In addition, most backup solutions perform a memory image backup or block data backup. In the simplest case, a signal is given to the system to be backed up to stop important processes for a short time and then access the file system directly at block level. In this way, you can back up volumes completely at the file system level. However, this is almost impossible when backing up databases during operation. For this reason, another technique is added to make it possible to record all blocks. For this purpose, all the blocks in the file system that are relevant for the backup are switched to read-only mode during operation and a small, previously empty, irrelevant area is defined for the data storage to be written into. In this way, no data is lost, and the backup software can back up all blocks of the file system. After the backup of these blocks has been completed, a second signal is issued to get the blocks out of read-only mode, and the data written during this time is integrated.

When using virtualization software, this system can be used much more easily because the "host" controls the guest system and knows the file system, making it possible for a "snapshot" of the guest (usually a server or client computer) to be created using the technology described above. The host is usually a central computer with permanent access. With a snapshot, all blocks of the guest's file system are simply switched to read-only mode and all write accesses are redirected to a separate area on the host. After the backup is complete, the snapshot can be removed, and all the written areas are automatically integrated. At this level, this works not only for the file system of the guest operating system but also for the main memory, which can then be integrated into the backup. This means that the complete status of the operating system of the guest computer is recorded in the backup during operation and is an immense advantage, especially for systems that need to be consistently available.

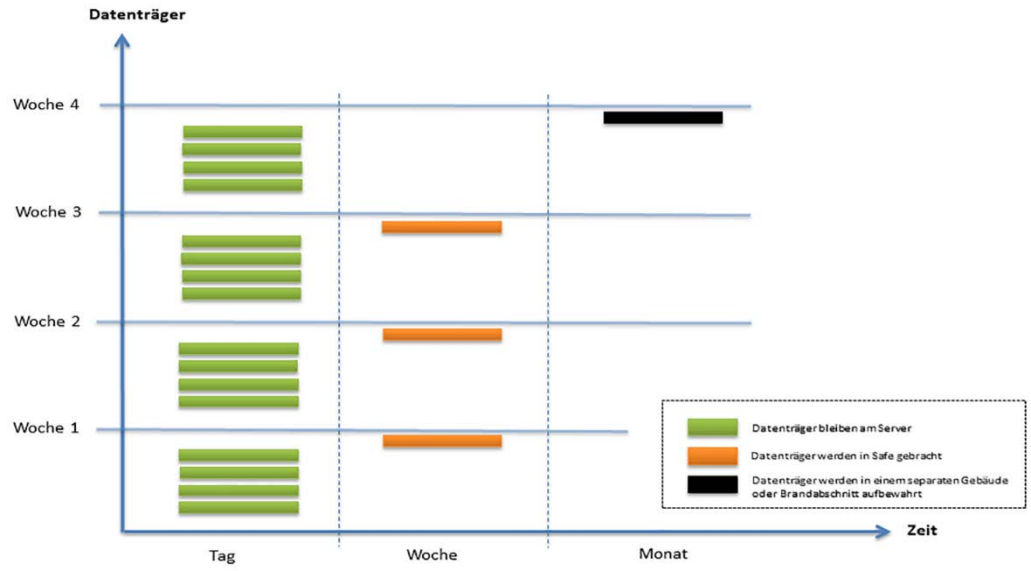


Fig. 108 Authors' sketch of the "generation principle" for data backups.

The “generation principle” in data backup is based on the idea that it makes sense to create several data backups at different times and then have them in stock. The organization must decide how many generations are created in total and include this in its data backup concept. Fig. 108 (read from right to left) shows an example whereby an overall data backup is carried out once a month and stored in a separate building or fire compartment. A corresponding data backup is also made at the beginning of a week and is kept in a safe. In the relevant weeks of the month, the institution’s database is backed up again every day and can be stored on the server. This approach limits any loss of data in the event of an attack or an emergency event.

Implementation and training exercises to raise awareness of IS

We consider it particularly important for ISOs to explore possible data backup strategies and the generation principle. This should certainly not just be a theoretical aspect of the training but needs to be actively practiced.

As an introduction to the exercise and discussions about data backup practices in the organization, we go back to the history (fig. 109). Using a kind of matrix, the characteristic features of data carriers are mapped to the distinct forms that have manifested over the centuries. The idea for this exercise was developed based on [77]. The specific features are assigned to the relevant modes of data recording and affixed to the board in the form of terms. We have deliberately made it a little easier by assigning colors, because this exercise should not take up a large amount of time but should be used instead to raise awareness.

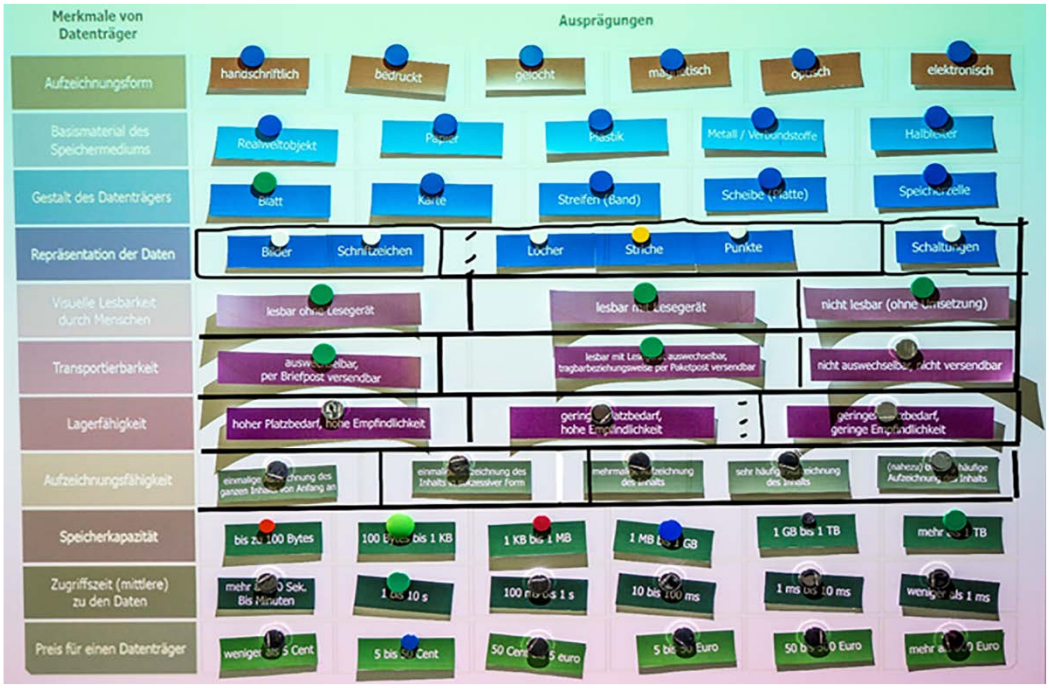


Fig. 109 Exercise to raise awareness of the criteria for selecting data storage media based on [77].

Since ISOs, as employees with specialist technical responsibilities, are responsible for reviewing a security concept, they must be included in the planning of an organization's data backup strategies. ISOs do not need to have the same technical background as administrators. Their job is to initiate, coordinate, and review. In order to equip them with the basic background knowledge of data backup strategies, the next step is an exercise that demonstrates the differences between full backup, differential backup, and incremental backup in a practical and comprehensible way. To carry out this exercise, the readers need a PC with Windows 10 and the Cobian Backup 11 software, which you can download free of charge from https://www.cobiansoft.com/ (April 2020). After installation, you will find the software in the system tray in the area of the hidden icons at bottom right. We start the exercise:

1. Open Cobian Backup, create the two folders *source* and *destination* on your desktop, and create two text files at random in the *source* folder. The *destination* folder also requires a subfolder for each backup type (fig. 110):
   a. Complete full backup
   b. Differential backup
   c. Incremental backup

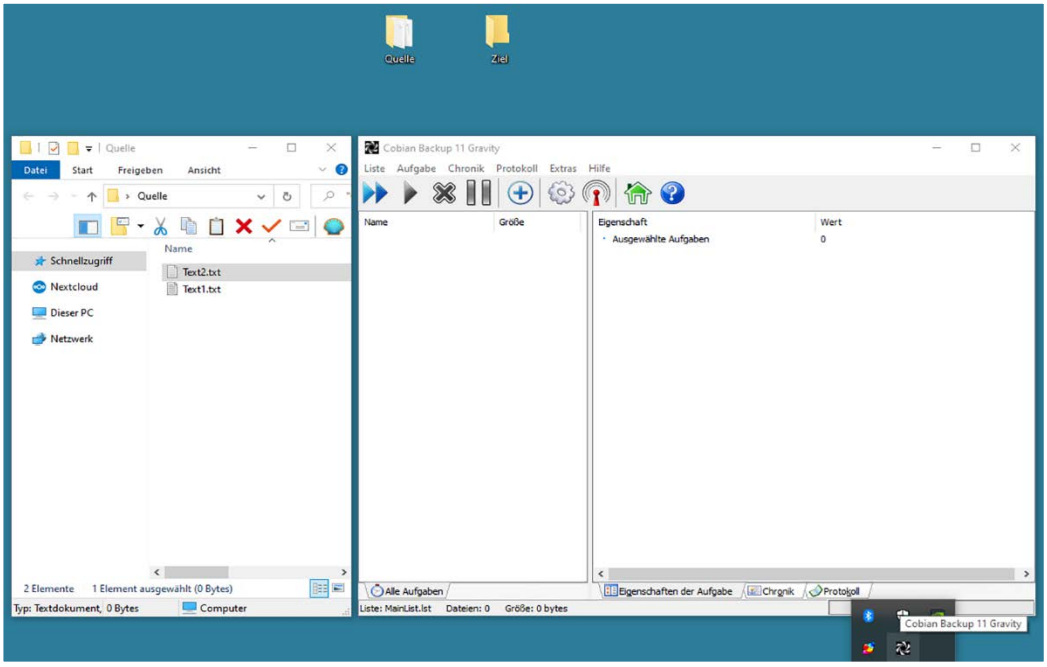


Fig. 110 Basic status of the backup software before starting the exercise.

2. As the first step of the data backup, a complete backup is created as a reference. To do this, a new backup task is created under the "Task" tab (fig. 111).

3. First, a full backup is created (fig. 112).

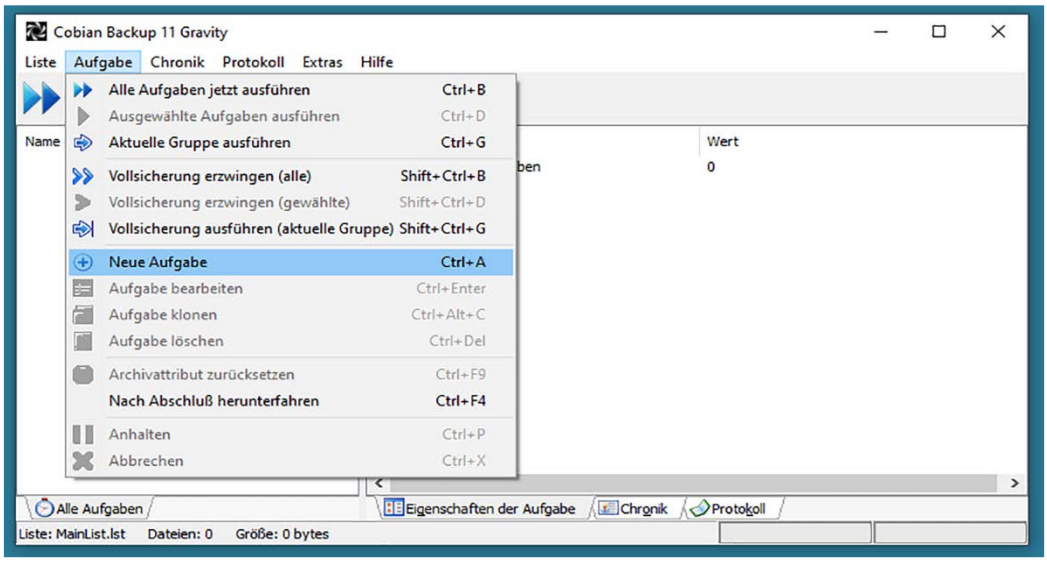


Fig. 111 Creating a new backup task.

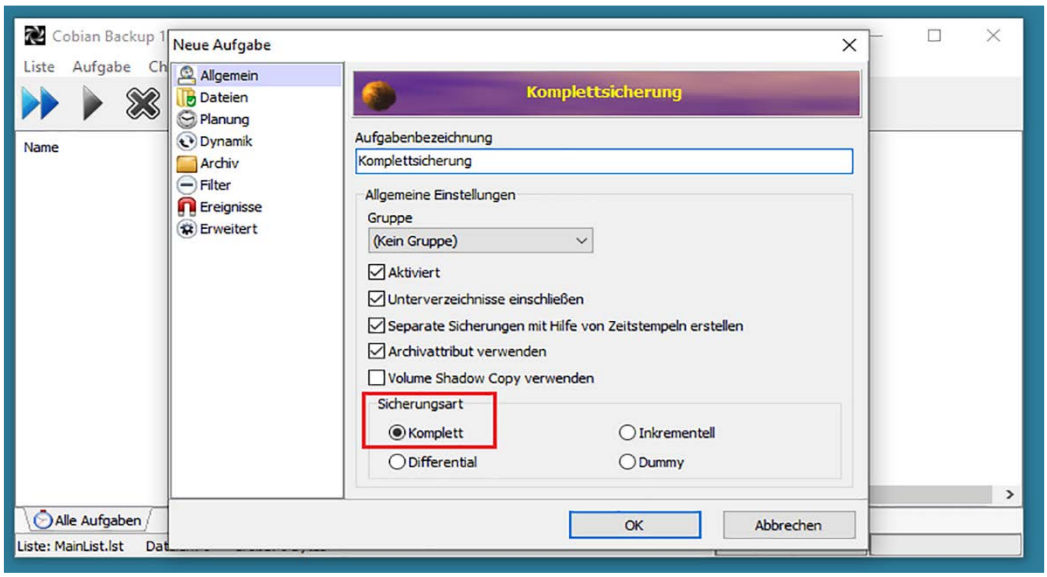


Fig. 112 Creating a new backup task: full data backup (complete).

4. In the “Files” submenu, our two folders *source* and *destination* are selected from the desktop using drag & drop. Make sure to adapt the *destination* folder to the backup type. For our full backup it is therefore `Desktop\Destination\Complete` under the user profile in question (fig. 113).

5. Make sure that the planning type is set to Manual in the “Planning” menu and confirm the task with OK (fig. 114).

6. Start the full backup by clicking on the triangle under the “Task” menu item. After the full backup has been carried out correctly, the folder `Desktop\Destination\Complete` should contain the first full backup (fig. 115).

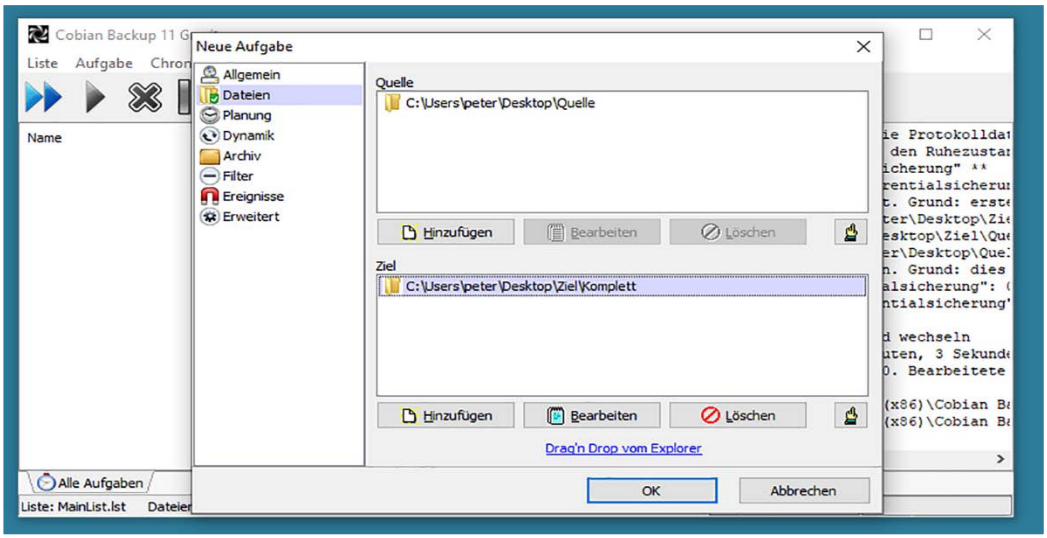


Fig. 113 Selection of "source" and "destination" from the desktop of the current user.

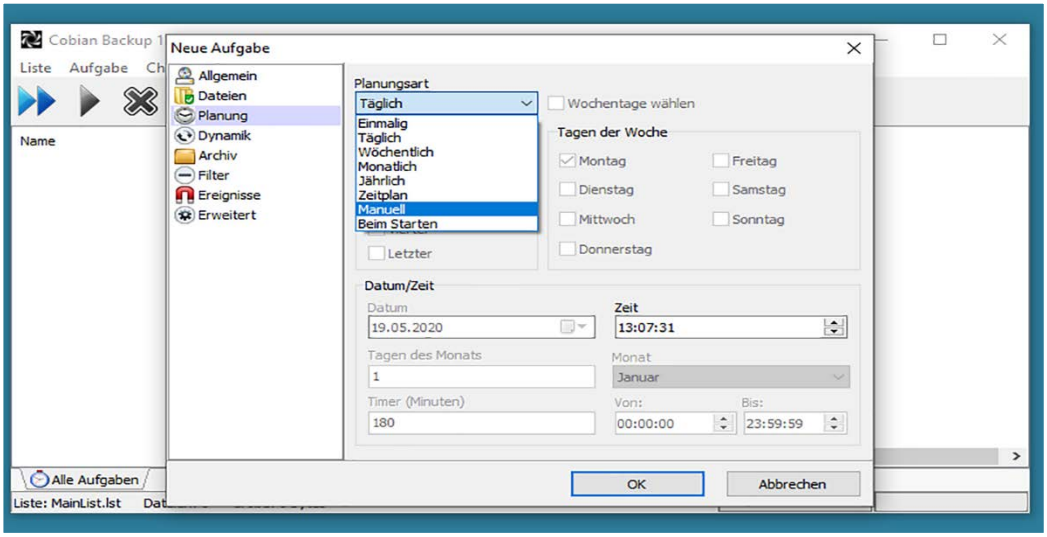


Fig. 114 Planning type set to "Manual" (in German: "Manuell").

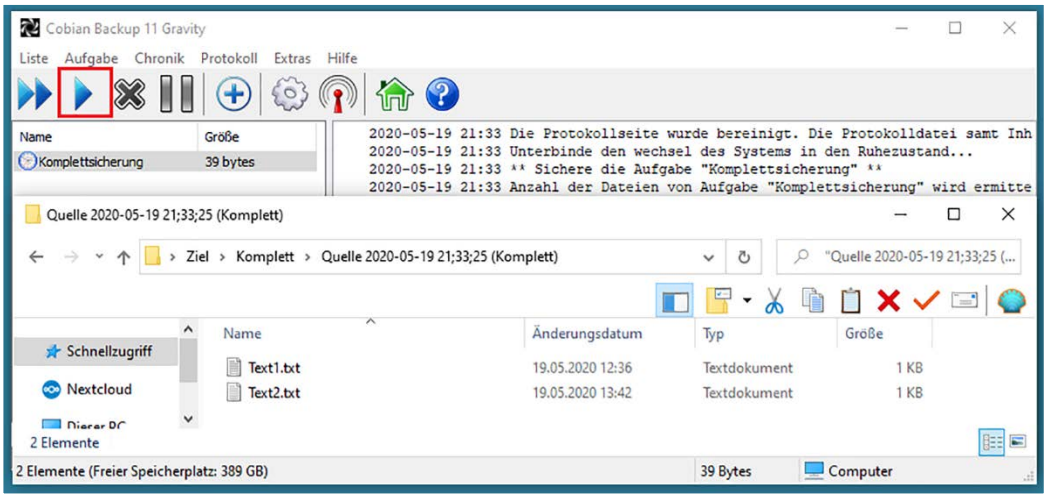


Fig. 115 Performing the first complete backup.

7. After the first successful full backup, add another Text3.txt file in the *source* folder (in German: “Quelle”) and start the full backup again (fig. 116):

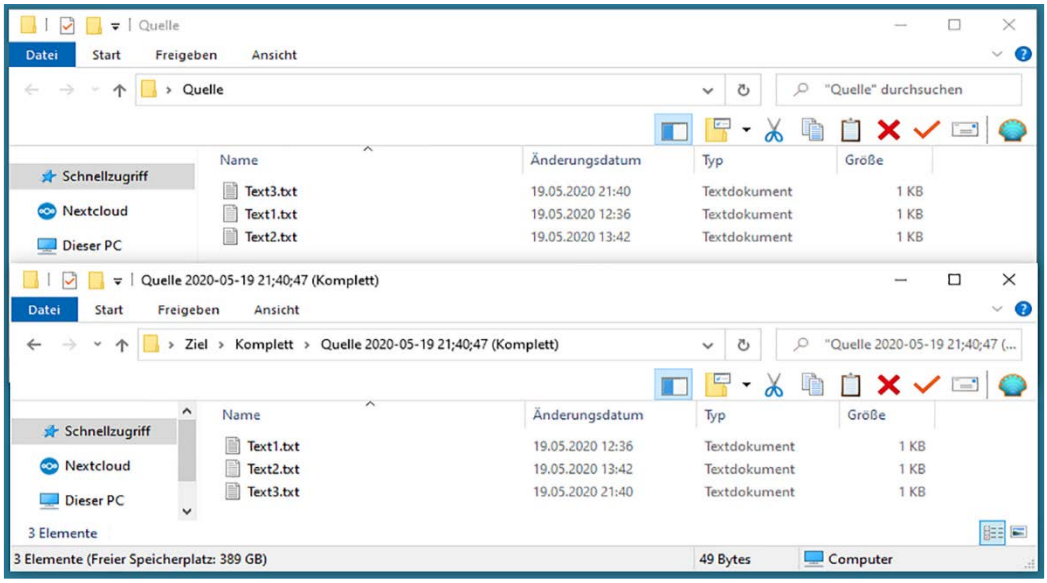


Fig. 116 Execution of the second complete backup.

8. As a final control step, please change the content of the Text2.txt file by a few characters and perform a complete backup again. As in the previous run, all files are recorded again, even if the data has not changed (like file Text1.txt), since the first backup (fig. 117):

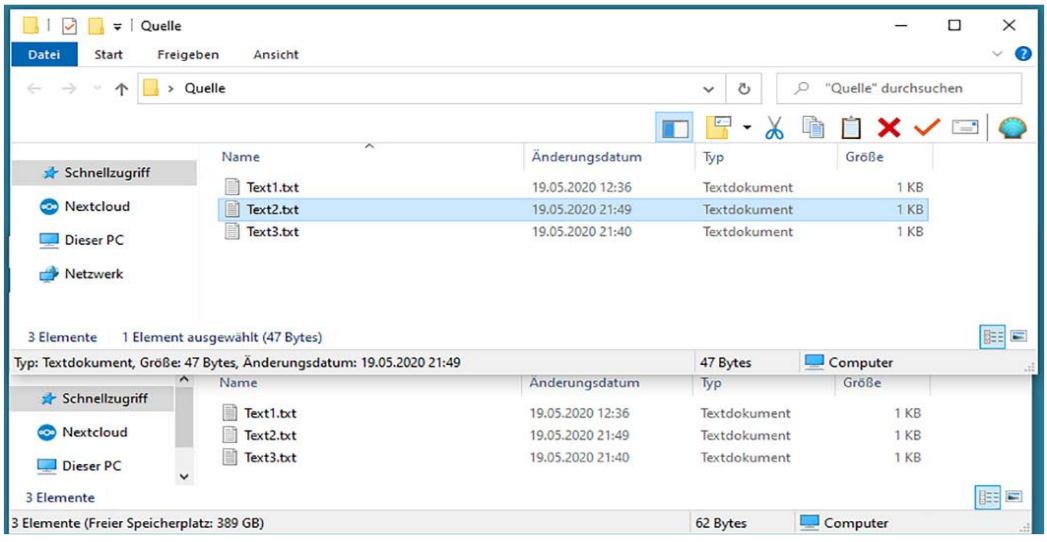


Fig. 117 Performing the third complete backup.

9. To show the differences to the incremental backup, please delete the Text3.txt file from the *source* folder and create an incremental backup following points 2 to 5 with the new *destination* folder `Desktop\Destination\Incremental` (fig. 118).

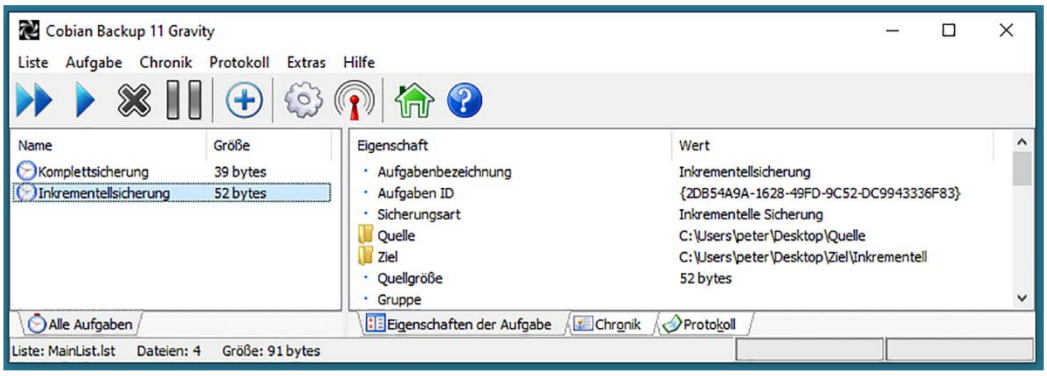


Fig. 118 Incremental backup in a new destination folder.

10. Now repeat steps 6, 7, and 8 with the incremental backup and compare the backup folders of the original full backup in each case (fig. 119):

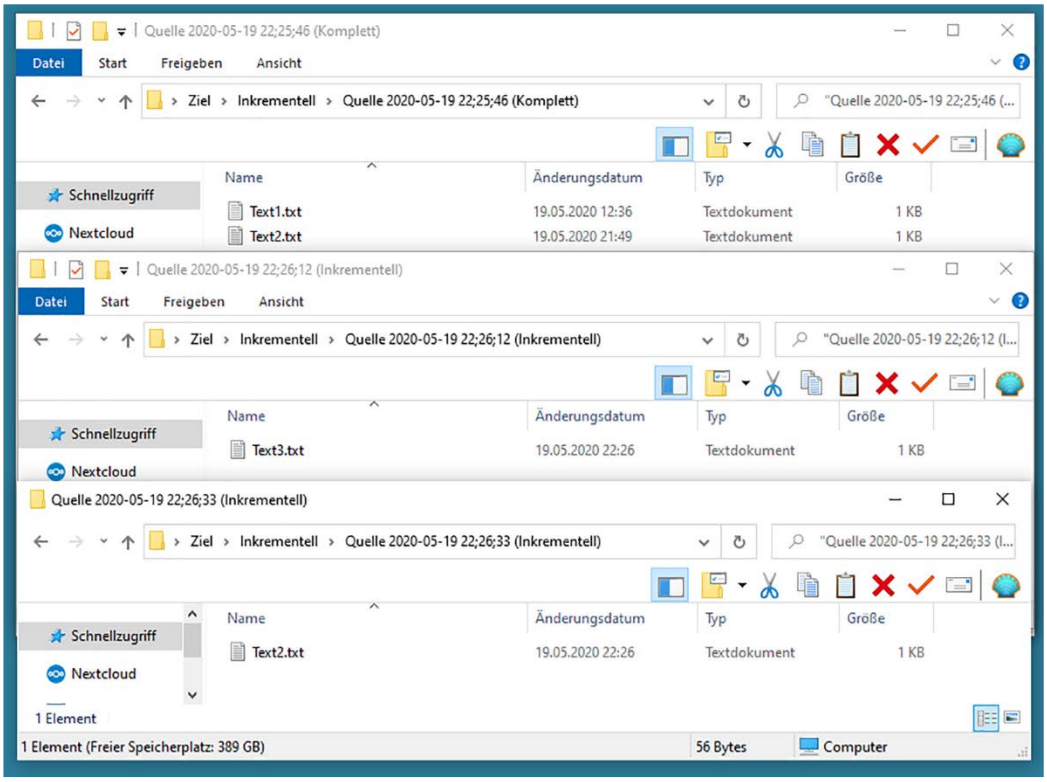


Fig. 119 Incremental backup in comparison.

As already described in the theoretical part, you can see from this process that an incremental backup basically only considers changes since the last backup. This is done without differentiating between a full backup and an incremental backup.

11. In order to display the differential backup, please delete the Text3.txt file from the source folder and create a differential backup following steps 2 to 5 with the new *destination* folder `Desktop\Destination\Differential` (fig. 120).

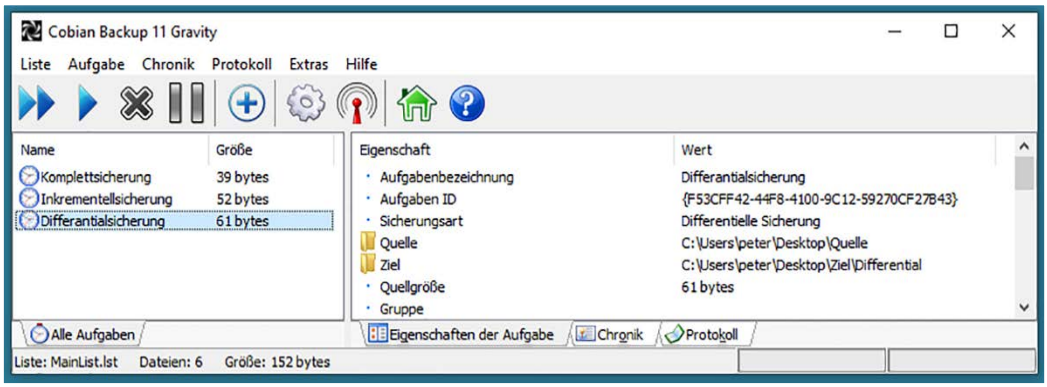


Fig. 120 Differential backup in a new destination folder.

12. Now repeat steps 6, 7, and 8 with the differential backup and compare the backup folders of the individual backups (fig. 121).

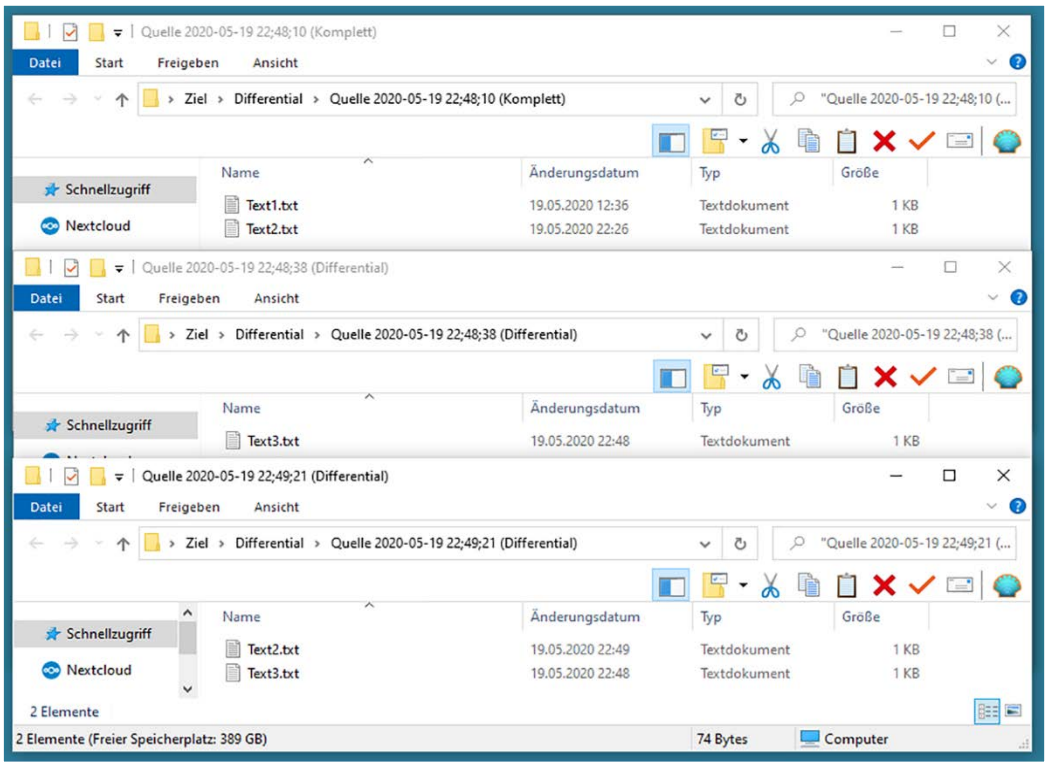


Fig. 121 Differential backup in comparison.

As described in the theoretical part, it can be seen from this process that a differential backup basically considers changes since the last full backup. Depending on the nature of the data in terms of file division or block division, as well as the volume and frequency of changes, these backup procedures must be planned carefully for the organization to enable the backup tasks to be optimized. In addition, by checking the amount of time involved, a framework can be defined for restoring any lost data.

Please test yourself with the following questions and comments on chapter 5.2:

- Can you identify the goal of a data backup strategy and explain the general concerns involved in such a concept?

- Can you explain the requirements for data backups to your colleagues?

- Complete the sentence: “The risk situation of a data backup concept contains the following aspects: …”

- Can you explain the difference between data backup and archiving?

- Can you explain the advantages and disadvantages of full data backups, differential backups, and incremental backups?

- Can you explain the generation principle in data backup?

- Identify criteria for selecting a particular data storage medium.

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

5.3 Software management, software vulnerabilities, and malware in a nutshell

The use of software is an integral part of our professional and private life. We can therefore assume that many people are now aware of the security problems associated with *malware*. Nonetheless, we note that users need to be much more conscious of this issue. Meanwhile, the dangers we know about are still a threat, because people's actions often do not tally with the recommendations of experts. In this chapter, we refer again to the BSI IT-Grundschutz, limiting ourselves once more to the essentials required by ISOs.

The term *software management* is often equated with the management of software projects. According to Balzert (2008) [78], software generally has special characteristics that make the management of software projects more difficult and cause them to fail if these features are ignored. "Compared to production processes, software development needs to be more closely managed, because software is invisible, the progress of development is difficult to determine, and ideas about the correct development process are still unclear" [78: 159]. In addition, according to Balzert [78], we need good software managers who can properly combine their general knowledge of management with their specialist knowledge of software technology. However, from the point of view of IT-Grundschutz, this complex area and the implications it has for security represent only one aspect of software management in today's institutional practice.

According to the *IT-Grundschutz Compendium* [20], the following modules are particularly relevant here:

- CON: *Conception and procedures*
    - CON.4 Selection and use of standard software [79]
    - CON.5 Development and use of individual software [80]
    - CON.8 Software development [81].
- OPS: *Operation*
    - OPS.1.1.3 Patch and change management [82]
    - OPS.1.1.4 Protection against malware [83]
    - OPS.1.1.6 Software tests and releases [84].
- Everything under APP: *Applications* [85]. At this point the focus is on
    - APP.1.1 Office products [86].

For the complex area described above, IT-Grundschutz takes into account the following risk situations with the module *CON.8 Software development* [81] and *CON.5 Development and use of individual software* [80]:

- Selection of an unsuitable procedural model
- Selection of an unsuitable development environment
- Lack of or inadequate quality assurance in the development process

- Lack of or inadequate documentation as well as undocumented functions
- Insufficiently secure use of development environments
- Software design errors
- Lack of or inadequate testing and approval procedures
- Software test with productive data
- Inadequate management of admission and access rights
- Inadequate contractual arrangements with external service providers
- Lack of or inadequate security measures in applications.

In addition, many institutions are concerned with the selection and use of standard software (see *CON.4* [79]). Office products are likely to make up a significant share in the use of standard software (see *APP1.1* [86]). IT-Grundschutz takes into account the following risk situations:

- Failure to adapt the standard software / office products to the needs of the institution
- Disclosure of sensitive information due to incorrect configuration
- Purchase of standard software / office products and updates from unreliable sources
- Software weaknesses in standard software / office products
- Use of unlicensed standard software / unlicensed office products
- Unauthorized exercise of rights in standard software / office products
- Loss of data due to incorrect use of standard software
- Data loss through password protection of Office documents
- Lack of or inadequate testing and approval procedures for Office products
- Data that should be protected in meta and residual information in Office documents
- Malicious content in Office documents
- Insufficient reliability of Office documents
- Loss of integrity of Office document.

In principle, the *IT operations* department is responsible for meeting these requirements, but ISOs must always be involved in the strategic decisions [86]. ISOs are also responsible for ensuring that all requirements are met and checked in accordance with the security concept that has been defined (see chapters 1 to 3). Users should be informed about the options and limits of the security functions in the software they have and the storage formats used in the standard protection procedure [86]. In addition, the requirements for the secure use of Office products should be integrated in the security policy. Under standard protection, all users should be made aware of the risks associated with meta and residual information (e.g., comments) in the products they use and trained in how they can remove residual information [86]. It is recommended that documents be sent in a format that cannot be changed if they do not require any processing by the recipient.

Even in the case of basic protection (see fig. 2), users must still be trained and made aware of how to deal with documents from external sources in line with IT-Grundschutz. The checking of documents from external sources should be enforced by technical measures according to the BSI [86].

According to *OPS.1.1.3 Patch and change management* [82] and *OPS.1.1.6 Software tests and releases* [84], the risk situations for IT operations are as follows:

- Poorly defined responsibilities
- Poor communication in change management
- Insufficient consideration of business processes and specialist tasks
- Insufficient resources in patch and change management
- Problems with the automated distribution of patches and changes
- Poor recovery options in patch and change management
- Insufficient consideration of mobile devices
- Inadequate contingency planning for patch and change management
- Misjudgment of the relevance of patches and changes
- Manipulation of data and tools in change management
- Incomplete implementation of the client's requirements
- Inadequate training of developers and software testers
- Software tests with productive data
- Lack of or inadequate testing procedure
- Lack of or insufficient approval procedure
- Lack of or insufficient documentation of the tests and test results
- Lack of or insufficient documentation of the release criteria.

For ISOs it should be noted that patch management is a special process within change management that targets the fixing of software bugs and weaknesses and must always be used [82]. In the individual system modules *SYS IT systems* and *APP Applications*, there are further requirements relating to patch management that is necessary in specific cases. *Patches* are to be distinguished from *updates* and *upgrades*: a patch is a fix from the manufacturer of the software to eliminate security gaps in the operating systems or application software and should be installed promptly.

ISOs should be familiar with the definition of malware, the different forms it takes, and how they work. The BAköV defines malware as any software "that contains undesired functions that can endanger—either unintentionally or deliberately—the availability of data, resources, or services and the confidentiality or integrity of data" [1]. The module *OPS.1.1.4 Protection against malicious programs* [83] in the BSI's IT-Grundschutz looks at the following threat situations:

- Software vulnerabilities and drive-by downloads
- Ransomware extortion
- Targeted attacks and social engineering

- Infections from mobile data carriers and other USB devices
- Botnets
- Infections of production systems and IoT devices.

Again, this module describes the general requirements for providing protection against malware. Specific requirements can be found in the individual modules.

This is especially the case for the system modules *SYS IT systems*—e.g., in *SYS.2.2.3 Clients under Windows 10*. An identified malicious program can also lead to a security incident. In this case, the requirements of module *DER.2.1 Handling of security incidents* must also be taken into account. According to the BSI, the requirements of the module *DER.2.3 Cleaning up far-reaching security incidents* help to remove identified malicious programs and restore the system to a corrected state [83].

Implementation and training exercises to raise awareness of IS

As an initial awareness-raising measure, we present an exercise on the various types of malware and their mode of action, as developed by a student team from the Administrative Informatics program in the winter semester 2018/19 [87] (see fig. 122).

The learning scenario [87] is a quiz whose aim is to get a team to work together to engage with the topic of malware. Everyday and special situations that can endanger IS are described in a playful way. In addition, reference is made to the functionality of the malware and historical examples, which are not only intriguing but also instructive [87]. In the competition, three teams of around three people compete to answer the fifty questions. The game is scalable by reducing the number of quiz questions. The team members should discuss the quiz questions, come up with plausible solutions, and then place the colored answer cards A, B, C (green, red, blue) accordingly. The exchange of ideas helps consolidate individual knowledge while also introducing new ideas.

In addition to the fifty quiz cards, each team has three point cards in the team colors, and there are a total of twelve joker cards. Quiz cards and joker cards are each shuffled and placed separately face down on the desk.

The moderator reads the first question aloud in a clear voice. Only when the question has been read out completely are the three teams allowed to place their answer card face down in the middle—they have ten seconds in which to do this. It is not about the speed at which the answer cards are placed in the middle of the table—the only thing that counts is whether the answer is correct. Then the cards are turned over and the moderator assesses the answers. If a team has the wrong answer, it must hand over one of its point cards and may draw a joker card in return [87].

Fig. 122 "Malware"—analog game-based learning scenario for three teams. Developed in the first semester of the Information Security and Awareness (ISA) course in the Administrative Informatics program (VIBB-18) at TH Wildau. Concept, design, and production by the group Lukas Dorn, Henrik Koschel, Jonas Lang, Steven Müller, Jonas Thiem, and Vincent Westphal, January 2019. The symbols used on the cards are part of "Font Awesome" from Fonticons, Inc., and are licensed under CC BY 4.0 [87].

The joker cards can be used for one of the next questions and lead to other interesting game dynamics. Their functions are as follows:

- "Trojan" joker: The team can take a point card from the other team (with the most point cards).
- "Spyware" joker: The team may view another team's answer.
- "Virus" joker: If another team answers the question incorrectly, it loses two point cards. If none of the groups answered the question incorrectly, nothing happens.
- "Antivirus program" joker: This negates the effect of a joker. This card can therefore only be played if another team has played a joker.
- "System update" joker: One of the incorrect options is resolved. If this joker is played, the moderator shows one of the wrong answers to the team playing the card.
- "Firewall" joker: The team does not lose a point card if its answer is wrong.

The second awareness-raising scenario deals with the topic of "Using video games safely," another exercise idea from the first semester ISA course in the Administrative Informatics program (VIBB-18) in the winter semester 2018/19 [88]. It is possible that one or the other ISO thinks that this topic is not so relevant in the operational context. There are two reasons why such topics can also play a role in awareness-raising measures. We know from research that the more sustainable measures are, the more they can be used in private life. In addition, many employees have children who play such games with passion and who may buy items, which means that parental supervision is important.

This game (fig. 123) is also structured as a card game with questions: answering these questions requires in-depth discussion between the participants. But what is actually included in video games?

The learning scenario's student development team counted everything connected with the actual games as well as the associated forums [88]. For example, *Steam*, the largest digital platform for video games, does not only give people the opportunity to play video games, it also creates communities and shares artwork. Such platforms make playing games with friends on the Internet much easier and more attractive. The Steam platform has changed over the last years to become more of a social platform. Negative aspects may also come to light: the changes make it easier for participants to be scammed—i.e., through abuses in the trading of avatar skills.

For example, a valuable knife from the *Counter-Strike Global Offensive* may be put up for trade, but the scammer pretends to have a disconnect, a connection breakdown to the server. If he or she comes back to do the deal later, the high-quality and expensive knife may have been replaced by a knife of lower quality that looks the same [88]. Now you may ask, "So what?," but if such frauds are not recognized, it can mean a loss of several hundred euros for the person being cheated.

Fig. 123 *"Use video games safely in a secure manner"—an analog game-based learning scenario. Developed in the first semester of the Information Security and Awareness (ISA) course in the Administrative Informatics program (VIBB-18) at TH Wildau. Concept, design, and production by Philip Szukala, Dustin Lohse, and Florian Makus, January 2019. The back of the card was designed by a photographer named Tookapic, who publishes this image on Pexels under the CC0 (Creative Commons Zero) license and for use in commercial and noncommercial projects [88].*

We know from psychology-based research on company awareness that it is interesting for participants in awareness-raising measures to understand the motivation and effectiveness of the attacker. Usually such attacks propose lucrative "business models," which are designed to generate large amounts of money. An awareness-raising measure sticks more easily in the memory of the participants when they slip into the role of the attackers themselves. We would like to illustrate this with the following software-based exercise dealing with an old software security gap. First of all, it should be pointed out that the exercise does not violate the German StGB § 202c, the so-called hacker paragraph, which there has been a lot of discussion of. As was made clear in 2009 by the legal committee of the German Bundestag and the Ministry of Justice, on the one hand, and the German Federal Constitutional Court on the other, this paragraph would be violated if software is developed or modified with the intention of spying on data (StGB § 202a) or for the purposes of intercepting data (StGB § 202b) (see [89]). This is in no way the intention of the following demonstration exercise. Rather, it is about clarifying how software vulnerabilities can be exploited.

As a third awareness-raising scenario, the following demonstration exercise looks at the very old security vulnerability CVE-2014-6332 from 2014, which presents the basic vulnerability allowing the standard mechanisms in Microsoft operating systems to be exploited. This exercise does not demonstrate current problems but illustrates the fundamental danger posed by standard processes and supplied interfaces that can be attacked. In our opinion, this old security gap gives a striking demonstration of this. Owing to its age and the fact that it is limited to the 32-bit edition of Windows 7, it is completely harmless for modern operating systems and can also be implemented by laypeople. The main source code used is listed on many other websites and is available for download—for example, on GitHub (see [90]).

If you want to technically replicate the following exercise, various basic requirements must be met, which are not discussed further in this book:

- In the demonstration exercise, we assume that a Windows 7 (32-bit) system virtualized with the VMware Workstation Player in a patch version of 2013 is installed. In addition, a local web server and a simple editor are installed, such as Notepad ++ and a trial version of Winrar (old version 5.21.).
- If you want to work with the code, we recommend that you use a separate computer as a security measure. You should disconnect the computer from the network after downloading all the necessary software products and the actual CVE-2014-6332 source code. Since the code is recognized by every current virus scanner, alarm messages and deletion or quarantining can be expected.
- The security vulnerability considered here enables remote code execution because the version of Internet Explorer (IE) that is used cannot properly handle access to objects in the memory. This is known as buffer overflow.

In the case shown, the IE integrated in Windows 7 is used for the attack, and the buffer overflow could be triggered by a simple Visual Basic Script (VBScript). This made targeted attacks possible, also for users of the operating system who did not use the software IE that was the focus of the attack.

1. The first screenshot shows our starting point. In addition to the software mentioned above, there is a text file and a folder link to the installed web server you will require. For the sake of simplicity, the web server is installed directly on the demo device and filled with the three files from the download. For this reason, there is also a reference to http://127.0.0.1/test.html (fig. 124). The source text of the HTML reference is:

```
<html><head><title>CVE20146332Demo</title>
<META http-equiv="refresh" content="0;
URL=http://127.0.0.1/test.html">
</head></html>
```

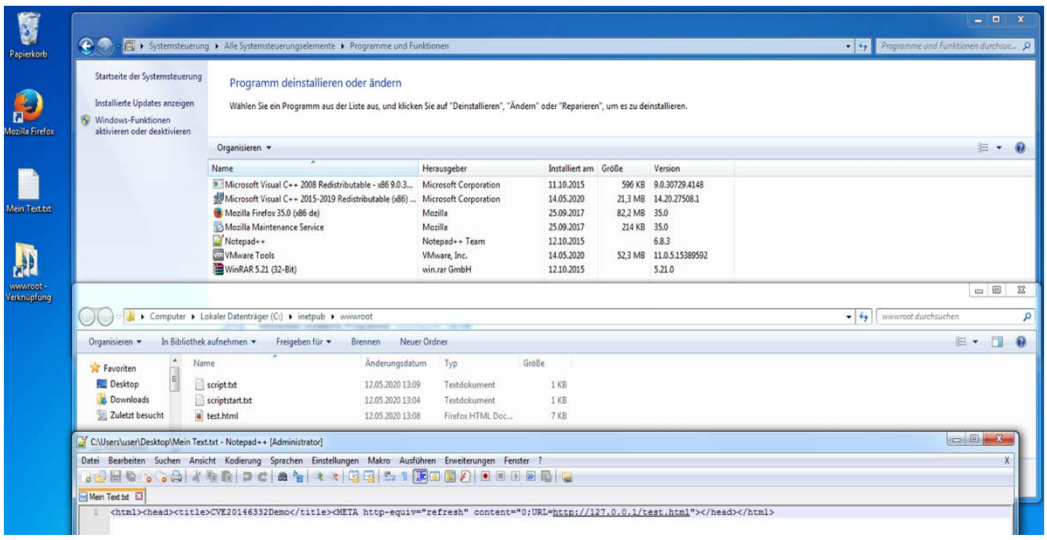


Fig. 124 Basic state of the Windows 7 installation.

2. The aim is to execute this source text as code via the IE of the computer under attack. Since almost no one uses this browser anymore, we package the code before sending it to the alleged victim: this forces it be executed in IE. To do this, we first put the source text from the file on the clipboard (Ctrl + C) for later use. Then we create a new document with the help of Winrar by right-clicking on the text file using “Add to Archive” (in German: “Zum Archiv hinzufügen”) (fig. 125).

3. To create an executable file, we mark the corresponding option in Winrar and then switch to the “Advanced” tab (in German: “Erweitert”) (fig. 126).

4. In the “Advanced” tab, switch to “SFX options” (fig. 127) and then to the “Text and Icon” area (fig. 128).

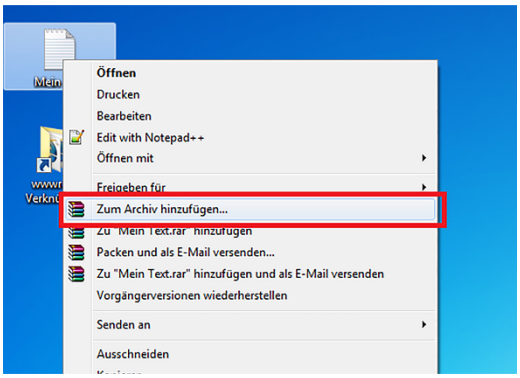


Fig. 125 Create archive with Winrar.

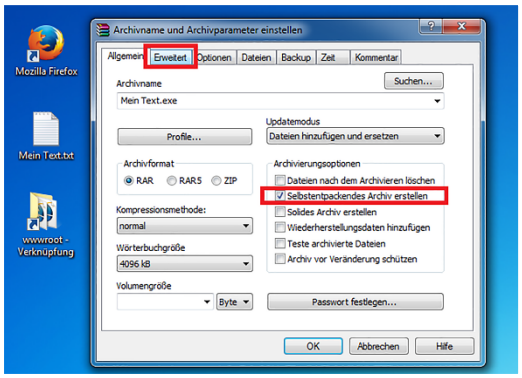


Fig. 126 Create self-extracting archive with extended options.

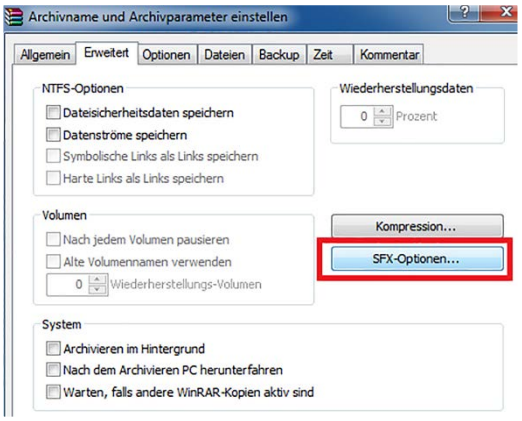


Fig. 127 Call up "SFX options."

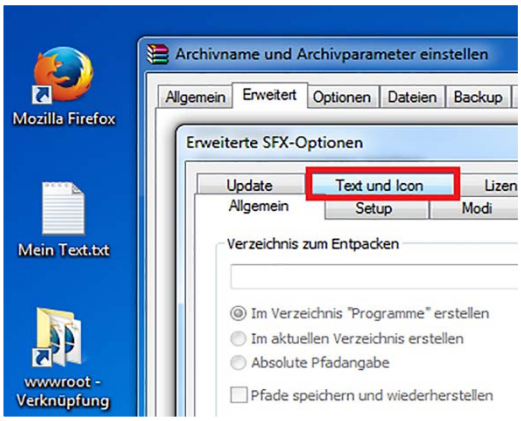


Fig. 128 Call up the "Text and Icon" tab.

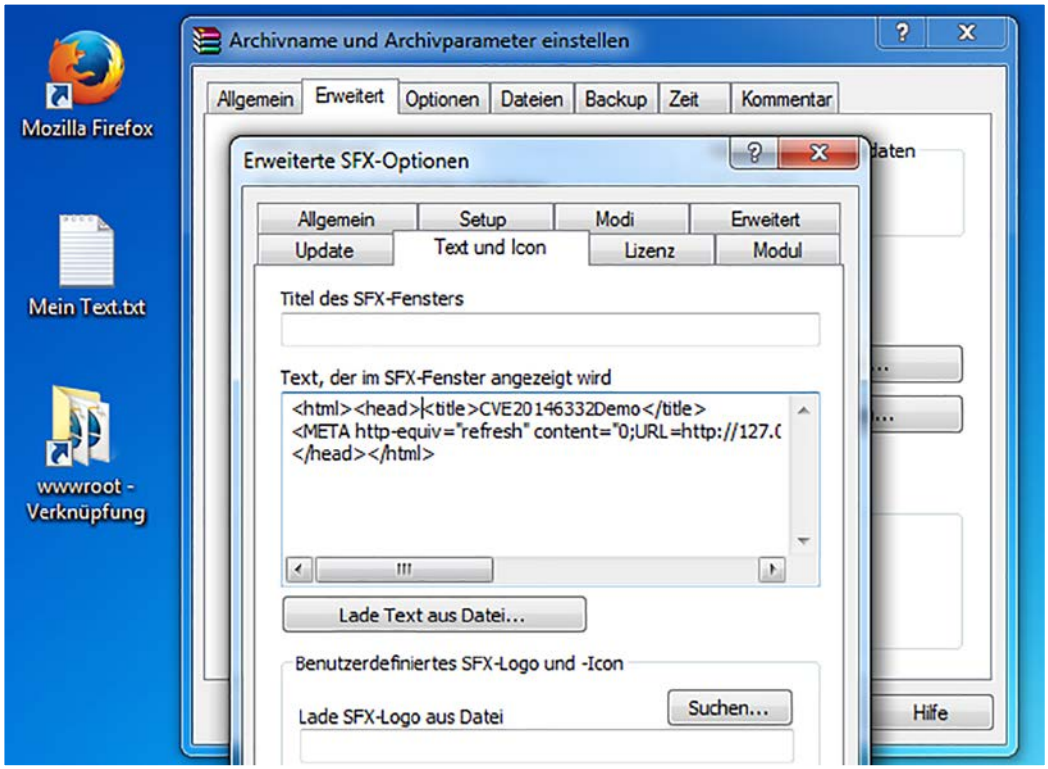


Fig. 129 Insert text and create executable file.

5. In the “Text and Icon” tab, we can now insert the text for calling up the website and then create the executable file with two clicks on OK (fig. 129).

6. Now run the “My Text.exe” file and watch what happens!

You will be able to see that two files have been placed on the desktop of the computer that were previously on the web server. In addition, one of the scripts was started. We only used the *Notepad* application for the harmless demonstration. If an attacker had, for example, used the partition manager instead, partitions might have been deleted in the system. In addition, other malicious code could simply be copied onto the system and then take full control of it.

Please test yourself with the following questions and comments on chapter 5.3:

- Explain the risk situations when selecting and using standard software, especially Office products.

- Explain why a lack of patch management leads to a threat.

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

5.4 Introduction to data protection for ISOs

In addition to running the advanced training course "IT security officers in public administration," which provides certification in cooperation with the BSI, the German Federal Academy of Public Administration (BAköV) also set up the advanced training course "Official data protection officers in the federal administration" a few years ago [91]. This qualification can also be completed with a five-year certificate and was developed in consultation with the Federal Commissioner for Data Protection (DP) and Freedom of Information (BfDI). In contrast to ISOs, the role of data protection officers (DPOs) has been legally implemented for decades and is mandatory for public administrations. Nevertheless, combined with increasing digitization, the work of DPOs has continued to gain in importance. In addition to the European General Data Protection Regulation (GDPR), organizations are also governed by the Federal Data Protection Act, the respective state data protection laws, and data protection provisions set down in special laws. This book will not concern itself further with these aspects. Instead, we would simply like to clarify the important overlaps between information security and data security, on the one hand, and data protection on the other, to facilitate good cooperation between ISOs and DPOs based on a spirit of mutual confidence and trust.

DP is about personal data—i.e., information that identifies a person. The first data protection law was passed in Germany in 1970 in the state of Hessen. The judgment of the German Federal Constitutional Court of 1983 defined the basic right to informational self-determination. Since then, every individual citizen has, in principle, been able to determine for themself how their personal data is used and processed. The DP is thus the expression of the general right of personality. In contrast, IS serves to protect all the information in an organization.

The concept of "prohibition, except with authorization" applies to DP: i.e., the processing of personal data is fundamentally prohibited unless it has been explicitly authorized [91].

According to GDPR Art. 6, Para. 1, *Lawfulness of processing*, at least one of the following factors must also apply for processing to be legal [91] (see also [92]):

- Consent has been obtained from the person involved;
- Processing is necessary to perform a contract or implement pre-contractual measures;
- Processing is necessary to comply with a legal obligation;
- Processing is necessary to protect vital interests;
- Processing is necessary to perform a task in the public interest or in the exercise of official authority;
- Processing is necessary in pursuit of the parties' interest.

In evaluating the last point, consideration needs to be given to what carries more weight: safeguarding the legitimate interests of the data controller or the fundamental rights of the person involved.

According to the EU's GDPR, DP is based on the following principles [91] [92]: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity and confidentiality.

In *CON.2 Data protection* [93], which forms part of the module *CON Conception and procedures*, the BSI's updated *IT-Grundschutz Compendium* indicates the goal of the module, which is to connect the requirements of the standard data protection model (SDM) and IT-Grundschutz. The German data protection supervisory authorities call SDM an *operational method* for standardized data protection advice and testing practice, in particular with regard to the TOM in the GDPR (see [93]).

With the SDM, the required implementation of data protection regulations of Art. 5 of the GDPR [92] can be systematically monitored on the basis of seven data protection goals. The aim is to secure the

- availability,
- integrity,
- confidentiality,
- transparency,
- intervenability,
- non-linking of personal procedures, and
- overall requirement of data minimization [94].

In addition, the system resilience mentioned in GDPR Art. 32, Para. 1(b) [92] is seen as an additional requirement: this relies on specific properties in order to be able to meet the functional requirements derived from the data protection goals and the protective measures for processing activities (see also [94]).

Like IT-Grundschutz for IS, the SDM contains a list of generic modules as DP reference measures—these are being expanded successively. The first seven modules were published in September 2018 by the commissioners for data protection in the states of Hessen, Mecklenburg-Western Pomerania, Saxony, and Schleswig-Holstein, in conjunction with the German Evangelical Church [95]:

- SDM module 11 *Storage*
- SDM module 41 *Planning and specification*
- SDM module 42 *Documentation*
- SDM module 43 *Logging*
- SDM module 50 *Separation*
- SDM module 60 *Delete and destroy*
- SDM module 80 *Data protection management*.

In its module *CON.2 Data protection*, IT-Grundschutz lists the following two specific threats and weaknesses as a risk situation [93]:

- disregard of data protection laws or use of an incomplete risk model
- determining a protection requirement at too low a level

In addition, *G 0.18 Incorrect planning or lack of adaptation* is mentioned as an elementary risk.

The requirements of the module *CON.2 Data protection* in the *IT-Grundschutz Compendium* refer to the SDM methodology. The following *basic protection* (see fig. 2) must be implemented as a priority [93]:

- *CON.2.A1 Implementation of the standard data protection model (B)*. "The statutory provisions on data protection (GDPR, BDSG, and LDSG) MUST be observed. If the SDM methodology is not taken into account—i.e., the measures are not systematized on the basis of the data protection goals and compared with the reference measures catalog of the SDM—this SHOULD be justified and documented."

There are currently no additional requirements [93] for standard protection (see fig. 2) in addition to the basic protection requirements, which must be implemented in line with the latest technical specifications for the *CON.2 Data protection* module.

One source of conflict between ISO and DPO could be in the area of logging, which is used to perform a data-processing check retrospectively. In light of this, it is worth taking a closer look at the corresponding *SDM module 43 Logging* as an example [96]. In general, a log must be able to provide information about which instances of the organization (units, systems, or individuals) carried out what activity at a certain time, and which body of the organization kept the log. Logs are mostly created automatically but can also be created manually. Complete documentary proof is provided if the log data is valid, reliable, up to date, and complete.

However, according to *SDM module 43 Logging*, log data with a personal reference may only be evaluated for specified purposes and by specially authorized persons [96].

This data protection principle of purpose limitation applies to the logging of the activities of employees, administrative activities, and the activities of IT systems and interfaces. The regulations covering employee data protection also apply [96]. Log data may thus only be checked for the purposes that occasioned its storage [96]. This must be determined in advance.

To make it possible for data processing to be checked completely, *SDM module 43 Logging* [96] specifies that the following data be logged:

- time component (“When?”)
- instance that triggers an activity (“Who?”)
- activity or event that was triggered by the instance (“What?”)
- storage instance (source and destination) that stores this log data (“Logging by whom?”).

The deletion periods are also important for ISOs. According to SDM module *43 Logging* [96], two interrelated deletion periods are to be established: “Firstly, a deletion period based on technical requirements/relevance and, secondly, a deletion period applied for functional reasons at the particular logging level. The “technical” deletion period is the most important.” [96]

Implementation and training exercises to raise awareness of IS

The data protection law with all its articles and paragraphs can be a real challenge for non-lawyers in training courses. It is therefore important to relate specific aspects as much as possible to real life and practice. It should be clear from the brief description that logging, for example, is typically viewed differently by the two roles ISO and DPO: ISOs want the most extensive logging possible so that security incidents can be discovered in good time; DPOs are strictly concerned with the personal rights of the individuals involved and the legal basis for logging based on the idea of data minimization. The SDM is now integrated in the tools for security concepts. We favor the development of an exercise analogous to the tool-based security concept, according to chapter 3. We intend to develop and test such an exercise with the administrative informatics course in the winter semester 2020/21.

In the *SecAware4job* project [43], we as a research team had the board game “*Keep your data private. Every day.”* developed in German to raise awareness about data protection (see fig. 130). The background to this learning scenario is that, nowadays, people move much faster from place to place and make more extensive use of electronic services than in the past due to technological progress. However, there is an increasing risk of data loss or theft. To prevent this, special attention is required, coupled with an awareness of risk situations. The serious game contains scenarios for the areas of home (9x, symbolized by a couch), leisure (8x, symbolized by the fins), work (8x, symbolized by a laptop) and travel (11x, symbolized by a suitcase).

In the serious game there are also twenty-four protective measures cards and eleven reward cards with the ISO symbol [45]. The main aim of the board game is to question yourself about your individual behavior. With honest answers, you and your team should be made aware of how safe your individual behavior is.

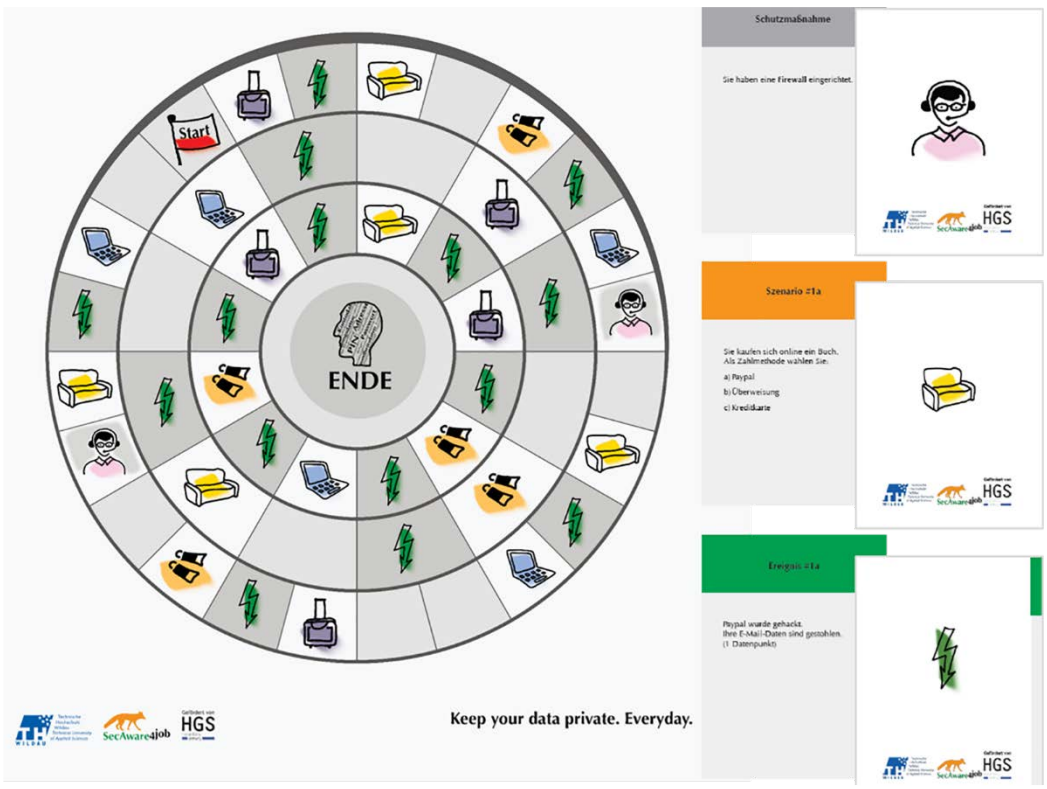


Fig. 130 Board game "Keep your data private. Everyday." developed by the Research Group Scholl at TH Wildau to raise awareness of data protection when using mobile devices and Internet services & apps (in German) [43] [45].

It should be noted that nowadays nobody can keep their personal data and private information 100 percent to themselves—in the game there are initially fifteen data points per person or team that can be gradually lost. Information has to be disclosed often in order to cope with everyday life. However, each person should know the risks and learn to control what data is disclosed and to what extent. The exchange of experiences is also very important here. As in real life, this board game is based on chance (roll of the dice, drawing of a card, etc.) and winning the game can even rely on a bit of luck. The game process can also be interrupted and evaluated at any time. The game instructions [97] explain the game process in detail (in German) and include a small glossary of the terms used.

In the gender-oriented project *Security* [46], an analog learning scenario on *image rights* was developed in two phases (in German). It can be borrowed from schools and used in the context of discussions on the DP (see fig. 131 and fig. 132). A three-stage digital online variant of this game is made available to the public in the project *SecAware4school* [51] (fig. 133).

In the first phase of the analog learning scenario (fig. 131), the aim is to impart knowledge about the *"Right to one's own image."*

This scenario should instill an awareness of which motifs can be photographed without asking permission and without reading house rules or similar documents. The first phase is thus about being able to apply a rationale for distinguishing between photos that can be taken without permission (green spread) and photos that cannot (red spread).

Fig. 131 Analog learning scenario for "Right to one's own image," developed in the "Security" project [46] [50].

Fig. 132 Analog learning scenario for copyright and CC licenses, developed in the "Security" project [46] [50].

The second phase (fig. 132) is about basic knowledge of copyright law—i.e., developing an awareness and understanding that images found on the Internet may not simply be used out of hand. In addition, knowledge about images that are in the public domain and the conditions governing their use should be imparted, with a particular focus on the Creative Commons (CC) license (see [98]). The CC symbols are clarified, and course participants have specific situations described to them out loud. Together, we consider the appropriate licensing for the photos on display to match the situation described. This learning scenario was very well received in a variety of tests in schools, at MINT events, and at the university.

In line with the task in the project SecAware4school [51] [52], the digital learning scenario was developed at three levels of difficulty (fig. 133) and can be accessed online via [99].

Fig. 133 Home page of the digital learning scenario on image rights (in German), which is publicly accessible and can be played at three levels of difficulty, developed in the "SecAware4school" project [99] [52].

There are a number of topics that are controversial from a DP point of view, and these are also dealt with juridically: these include data retention for the purpose of investigating and prosecuting serious crimes. There are enough pointers provided for this to enable ISOs to discuss the issue with management, employees, and DPOs. For DPOs, awareness-raising measures relating to DP are also important for employees, ISOs, and management. Ultimately, awareness-raising measures can be developed from all DP topics, whether it be on personal data protection and freedom of information, the directory of processing activities, order processing, or the data protection impact assessment. Sufficient materials are available for this purpose.

We show two examples from student projects where the primary focus is on *weighing interests*, with the idea of raising awareness about the subject of video surveillance in public and non-public spaces, and on the need to assess the various interests at stake. The first awareness-raising measure comes from André Bielig and Annika Hesse from the Brandenburg Public Administration program (ÖVBB-16). A total of fourteen scenes from everyday life situations were recorded in the form of pictures with short texts, and the question was asked as to whether video surveillance is permitted [100]. Again, the exchange between the participants is important, as is the justification of the result of weighing interests in light the GDPR, BDSG, and LDSG (fig. 134). The specific topics to be discussed focus on the following situations [100]:

- video-monitored staircases
- video-monitored outdoor seating on a publicly accessible sidewalk
- concealed surveillance of the employee break room in a company
- video-monitored factory workshop in a production company
- video-monitored children's bathing area at the swimming pool
- video-monitored trams and buses
- monitoring of building facades including public facilities (sidewalk, playground)
- monitoring of one's own property
- monitoring of the coat-check area in a restaurant
- night surveillance of a construction site to prevent theft
- video-monitored printer room in an institution.

Fig. 134 Raising awareness with photos about video surveillance [100].

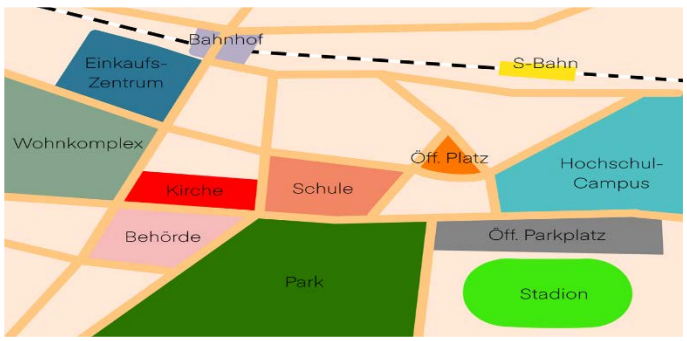


Fig. 135 Raising awareness of video surveillance using a map and stories [101].

The second awareness-raising measure on video surveillance was designed and implemented by Frederike Frank and Arvid Selle (also ÖVBB-16) [101]. Here, the texts for the situation were developed to correlate with a map (fig. 135). The question of how to balance personal interests with the legal situation is applied to a shopping center, train station, park, residential complex, school, public square, local authority, and stadium. ISOs and DPOs can also use simple means to jointly implement ideas like this for their specific organization, discussing the situations with the employees.

The following ideas were developed by student project teams in 2018 as a means to help course participants retain the content of the GDPR articles. One team is tasked with explaining Chapter VIII of the GDPR with a focus on Articles 83 and 84 [102]. The team developed the competition game "No. 83 NOT JUST A GAME—IT´S THE LAW" for two teams in English, where they have to answer questions on the general GDPR conditions relating to the imposition of fines and penalties (fig. 136).

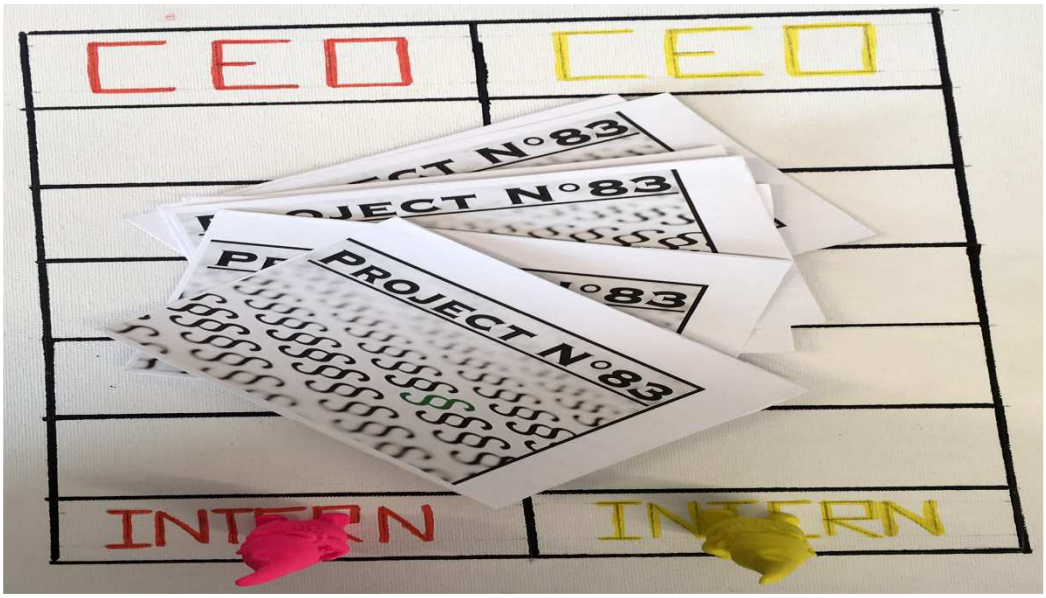


Fig. 136 Awareness-raising measure for the GDPR: Participants engage in a form of competition, with two teams having to answer questions on the GDPR. The analog serious game "No. 83 NOT JUST A GAME—IT'S THE LAW" was created in English by Idoia Cabañas, Victor Calderon, Sebastian Eppers, Sebastian Funk, Anton Raic, Emmanuel Kumi-Dumor, and Asya Urazbakhtina from the degree program "European Management Master" (EMM-17) as part of the project management course that ran in the winter semester 2017/18 [102].

Another student team from the European Management Master's degree program (EMM-17) designed an app for three key topics from the GDPR, Chapter III Art. 12–23 [103]: the *right of access* is based on Article 15; the *right to object* is based on Articles 17–19 and 21; and the *presentation of data* is based on Article 12. The learning scenario's introductory question, which relates to the number of EU member states, is shown in fig. 137. The results of the participants' survey could be viewed directly, together with the solutions, via a presentation medium.

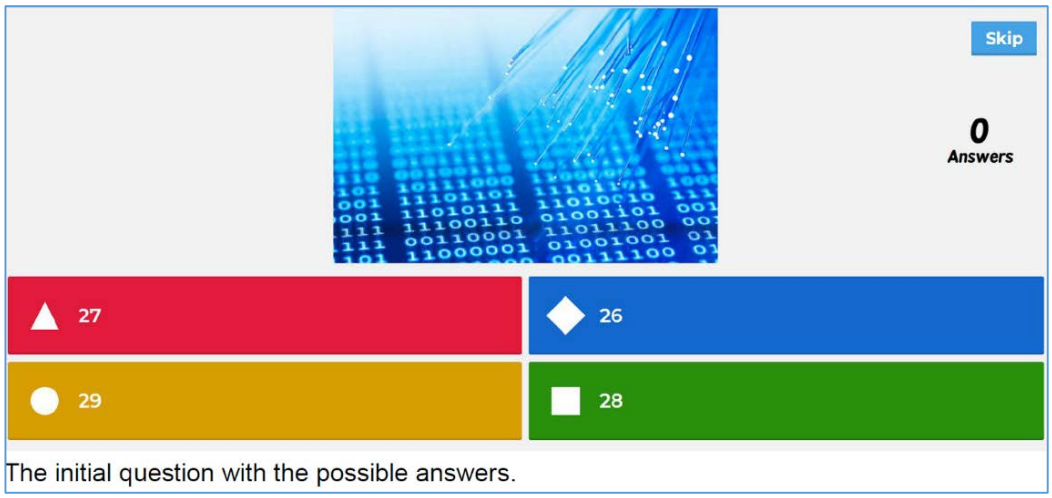


Fig. 137 Awareness-raising measure on the GDPR: All participants can see the answers and compare them with the solutions. The serious digital game was designed in English by Jessica Künkel, Isabelle Büge, Sabrina Udhardt, Marvin Brama, Esther Hüsing, and Gema Moquer Lopez from the European Management master's degree program (EMM-17) as part of the project management course that ran in the winter semester 2017/18 [103]. The opening question concerns the number of member states in the EU.

A further analog learning scenario, which was developed in English, dealt with the responsibilities for data protection activities set out in the GDPR (fig. 138); it concerns Chapter IV and Articles 24–43 [104]. The game deals with the terms *responsible person* and *jointly responsible person*, *data protection through technology design* and *data protection-friendly default settings*, *contract processors*, *directory of processing activities*, *data protection officer*, *supervisory authority*, and *certification bodies* (see [92]). The analog learning scenario makes use of fourteen questions or descriptions of situations, and answers must be assigned appropriately.

The fourth scenario, developed in English (fig. 139), focuses on Articles 6–8 of the GDPR—i.e., the *lawfulness of processing*, the *conditions for consent*, and *conditions for a child's consent* in relation to information society services [105]. Examples of the questions to be answered are:

- Will consent be given immediately if you willingly provide your data?
- If a student at TH Wildau fills out a questionnaire for another student, can the person concerned withdraw their consent to processing?
- If the data and consent are only given orally, is it legal for the controller to process the data?
- Can the government use your information without your consent?
- If a young person under the age of sixteen gives consent for their data to be processed, can this data be processed legally?
- Facebook offers you an online game that you can log into with your Facebook account. Facebook asks you for your consent to the use of your data. Can the game now use all of your information that is publicly shared on this platform?

Fig. 138 Awareness-raising measure on the GDPR: The analog scenario deals with the main responsibilities/roles involved in data protection. The serious game "Interactive teaching methods—Data protection" was created in English by Ege Özoktaş, Elangwe Halle, Fernando Carrasco, Hardep Aigner, Karolina Chomicka, Laura Zunk, and Ogün Kurt from the European Management master's degree program (EMM-17) as part of the project management course that ran in the winter semester 2017/18 [104].

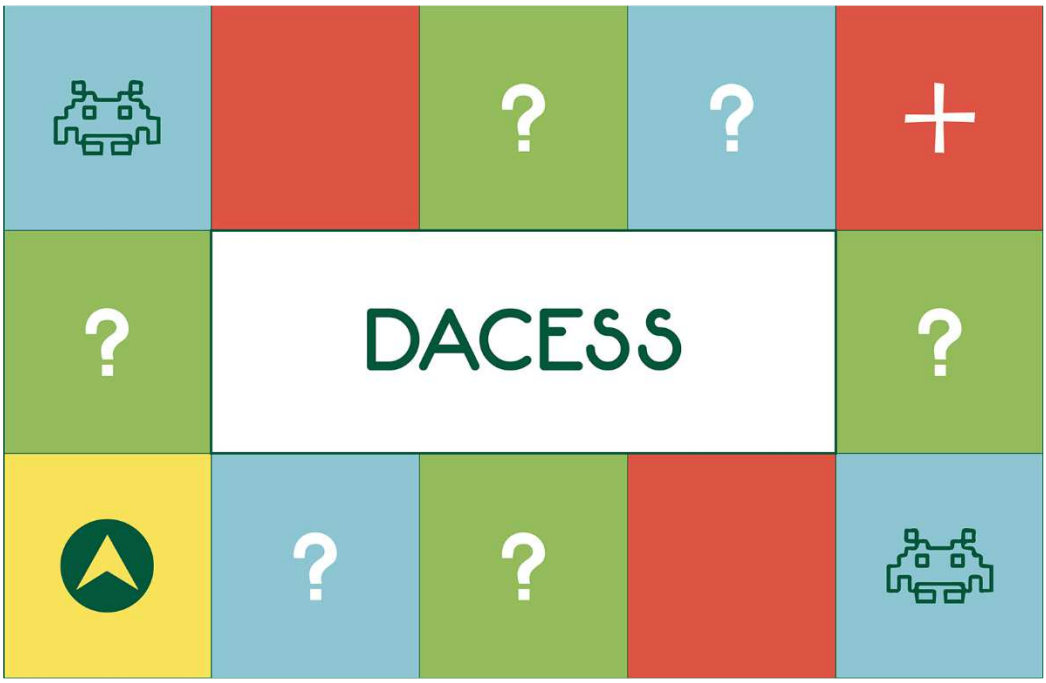


Fig. 139 Awareness-raising measure for the GDPR: Playing field of an analog scenario developed in English by Theresa Beran, Laura Pino Vanegas, Nathalia Calderon Scheel, Christin Schulz, Kimberly Henning, and Sarah Mandra from the European Management master's degree program (EMM-17) as part of the project management course that ran in in the winter semester 2017/18. Three players (or teams) draw cards and must correctly answer the questions about the EU's GDPR. The object of this game is to get as many points as possible [105].

As a final example from the student projects on data protection or GDPR, we will look at the following memory game [106]. ISOs and DPOs can easily create such awareness-raising measures in their own organization too (fig. 140). The learning scenario deals with Articles 63–84 of the GDPR with twenty-two question cards and twenty-two matching answer cards as well as four joker cards. The task is to find the pairs that match the content. The winner is the team that has the most matching card pairs. All cards can be dealt face down on a table, and the teams play a kind of "pseudo memory game"—played like this, the scenario can take a long time. However, the game can also be used flexibly: one option is to reduce the number of cards; another is to lay out the answer cards face up and ask the questions orally. Both these options reduce playing time.

Fig. 140 Awareness-raising measure for the GDPR: The analog memory game made up of question cards and answer cards was developed in German by Sven Baatz, Robert Rosinsky, Sebastian Freund, Christian Worm, Jennifer Hinterschuster, Katja Lehmann, and Danielle König from the "Administration and Law" degree program (VR-15) as part of the e-government project work course that ran in the winter semester 2017/18 [106].

Please test yourself using the following questions and comments for chapter 5.4:

- Can you explain the connection between the requirements for the standard data protection model (SDM) and IT-Grundschutz?

- Identify the seven data protection goals of the SDM methodology.

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

5.5 Networks in a nutshell

Nowadays, all organizations need secure IT and an appropriate network in order to function smoothly. Special attention to IS is necessary in institutions that are part of critical infrastructures. These are protected by the KRITIS Internet platform, which covers the public administrations of the federal, state, and local governments [107]. All of them have their own networks with different remits, structures, and levels of security. For example, the networks of the communities are to some extent integrated into those of the respective federal state, with some administrative districts organizing their own networks, while others rent them from IT service providers [108]. According to Article 91c of the Basic Law of Germany, all levels of the public administration are to be included in the federal network [108]. A secure infrastructure and thus network security must play a central role in all of them.

In order to comprehensively secure a network, those responsible for IT security have to make many decisions and carry out the proper configuration steps [109]. As is the case when securing and protecting company networks, public sector administrators have to plan and implement measures in line with the administrative body's security concept (see chapter 3). These include the configuration of firewalls, the establishment of a secure architecture to protect the internal network, the security of the mail and web server, and the selection of suitable antivirus solutions. In addition, there are connections to mobile workstations or end devices, and possibly entire branch offices via virtual private networks (VPN).

Since ISOs have to manage the implementation of the relevant measures in alignment with the security concept that has been devised, it is important that they have a technical background in networks. It is also useful for them to have theoretical knowledge of the Open System Interconnection (OSI) layer model covering electronic communication: this model was standardized internationally in 1983. As this background knowledge is extremely diverse and extensive, we point to appropriate training courses for ISOs. For the purposes of this book, we will limit ourselves to the essentials.

ISOs should have knowledge of the safe operation of network components. This includes knowledge of

- the functionality of switches and routers,
- the establishment of virtual networks (VLAN),
- the tasks, components, and basic architecture of a firewall,
- personal firewalls (as necessary),
- the goals, protocols, and security measures pertaining to the use of virtual private networks (VPN),

- the types and areas of application of wireless technologies like WLAN, Bluetooth, and NFC,
- mobile devices, and
- virtualization (where applicable).

Routers and switches form the backbone of today's IT networks according to the *IT-Grundschutz Compendium* module *NET.3.1 Routers and switches*, whereby the functions of switches and routers, which were originally different, are nowadays often combined on one device [111]. Routers work on OSI layer 3 (the network layer) and transfer data packets based on the destination IP (Internet Protocol) address in the IP header [111]. Routers are able to connect networks with different topographies. A router identifies a suitable connection between the source system (or source network) and the destination system (or destination network) and typically forwards the data packets to the next router [111]. Virtual networks (VLAN) can be used to restrict data traffic in a network coupled by switches [1]. The VLAN is a logical subnet of workstations and servers that belong together in a physical network and should not be confused with VPN. VLANs offer a large number of attack points, which is why VLANs with different protection requirements should not be configured on a switch [1].

A *firewall* is a system of software and hardware components that securely couples IP-based data networks [112]. *Secure* means that only the desired accesses or data streams between different networks are permitted. For this purpose, *filter lists* are used to define what electronic communication is allowed and what is not. These days, single components are typically not used in isolation to secure network transitions. Rather, a whole series of IT systems take on different tasks: these may be exclusively focused on filtering packets or act to strictly separate network connections using proxy functionality [112]. One requirement of basic security is that clients and servers must be placed in different security segments, and that communication between these segments must be controlled at least by a stateful packet filter (firewall) [113].

With the help of a *VPN*, data can be transmitted over untrustworthy networks such as the Internet in a protected manner using cryptographic procedures, while maintaining their integrity and confidentiality. A VPN is a network that is physically operated within another network but is logically separated from this network [114]. VPNs are an additional connection that employees should use, especially when working in a mobile context in insecure environments [115].

A *WLAN* is a wireless local area network, based on the international standard IEEE 802.11 and its supplements. Because they are usually quick and easy to install, WLANs are used to set up temporary networks—for example, at trade fairs or smaller events [116]. In the meantime, such networks are also offered in public places (airports, train stations, etc.) via so-called hotspots, which enable users to connect to the Internet or their institutional

network [116]. These networks are usually configured as *open* in public places, which is why such networks should not be used without VPN.

At this point, we pass on the recommendations of the BAköV [1] on the topic of networks with regard to the BSI IT Grundschutz. Accordingly, ISOs should consider the following modules of the *IT-Grundschutz Compendium*:

- NET.3.1 Routers and switches [111]
- NET.3.2 Firewalls [112]
- Net.3.3 VPNs [114]
- NET.2.1 WLAN operation [116]
- NET.2.2 WLAN usage
- SYS.3.1 Laptops
- SYS.3.2.1 General smartphones and tablets
- SYS.3.2.2 Mobile Device Management (MDM)
- SYS.3.2.3 iOS (for Enterprise)
- SYS.3.2.4 Android
- SYS.3.4 Mobile data carriers
- INF.9 Mobile workstations [115]
- SYS.1.5 Virtualization
- SYS.1.8 Storage solutions
- NET.1.1 Network architecture [113]
- NET.1.2 Network management.

Readers will find a number of modules to read on the extensive topic of networks in both the old and the modernized IT-Grundschutz. To finish, we would like to explain two aspects in more detail: firstly, the different *types of filters* and on, secondly, *pharming* attacks.

As already indicated above, different types of filter are required at various points when setting up secure networks. One well-known variety serves to filter emails containing unwanted advertising, called spam. Distinction is made between the following filter types [1]:

- Blacklist:
  Access is denied based on the expressions defined in a list (syllables, words, email addresses).
- Whitelist:
  Here, for example, only those email addresses that appear on a list of approved senders are accepted.
- Graylist:
  If the sender is unknown, the email may be initially rejected and only forwarded to the addressees on the second attempt by the sending mail server.
- Bayesian filter:
  This is a self-learning filter that operates on the basis of probabilities.

- Database:
  An attempt is made to identify typical characteristics, for example, of all spam emails. Such features or their hash values are stored in a data pool.

Pharming is a form of attack based on a manipulated "translation" of a computer name to an IP address. The background to this is the Domain Name System (DNS) used to translate domain names into the Uniform Resource Locators (URL) that allow us to browse the World Wide Web. A URL, such as www.th-wildau.de, is more understandable for humans than an IP address. However, this URL must be translated into the (static) IP address of the server that has been dialed up via a DNS server. Attackers try to manipulate this "translation." The result of a manipulation is that the users of a website think they are on the correct page and enter their login data, when in fact they are entering this data into a (possibly very good) fake website on a completely different server. The data can then be used by the attacker on the real website.

Implementation and training exercises to raise awareness of IS

We presented the learning scenario we developed as a means to discuss the possible structure of a secure network architecture in fig. 90 (chapter 4). For example, course participants can exchange ideas about one-level firewall structures with a packet filter or multi-level structures with two packet filters, an application level gateway (ALG), and three connected "demilitarized zones" (DMZ). The positions of the VPN remote stations protected by packet filters can also be illustrated. In our advanced training, we have had very good experience with this learning scenario, especially for participants who are not technically oriented. The participants achieved a fundamental understanding of the architecture background.

Moreover, if an institution is using mail and web servers, it must be prepared for DoS or DDoS attacks that seek to prevent the provision of services. The abbreviation stands for (Distributed) Denial of Service and often uses so-called botnets to disable the services of the computer system under attack. In order to be able to generate the required quantity and quality of queries, a large number of computers are required. These are associations of hijacked computers that attackers can remotely control at the appropriate time using previously installed malware, so that, for example, a flood of spam mails can be initiated for the computer system that has been targeted. Nowadays, botnets are also professionally leased.

Our question that came up in the process of developing learning scenarios was how this DDoS attack could be presented as an *analog* scenario? Stephan Gebur's bachelor thesis provided the answer (fig. 141). His basic idea involves a "user team" playing against an "attacker team" in three rounds [117]. A funnel, which represents the server being attacked, was chosen as the basis of the learning scenario. The team's data requests to this

server are represented by little balls: the user team has white balls and the attacking team has black balls, which are to be placed in the upper part of the game. The white and black balls are supposed to represent the data requests to the server. In order to show the availability of the service, the balls are channeled into a closed tube after passing through the funnel [117] (fig. 142). This should provide an exact reading to show which balls went through the funnel first [117]. The game instructions assist the attacking team from round to round so that at the end, despite the random principle at work, the effect is clearly visible to the participants: the black balls block access. The learning scenario is about raising awareness and not about technical subtleties.

Fig. 141 Analog learning scenario DDoS from Mr. S. Gebur [117].

Fig. 142 Example of the result of one of the rounds of the analog game DDoS [117].

The risks of Internet services and apps are dealt with in a learning scenario of the same name from the “Security Arena” produced by the firm known_sense [39] (fig. 143), which we can recommend for anyone seeking to develop appropriate risk assessment. Its additional special feature is that the “solution” changes over time, as the service providers modify both their services and their terms and conditions. The basic principle of the scenario is enacted in two phases: in the first phase, the icons of the examples for services are assigned; in the second phase, the risks for all services are discussed and, if relevant, marked with a chip. It quickly becomes clear to the participants what and how many risks are associated with the use of such Internet services and apps.

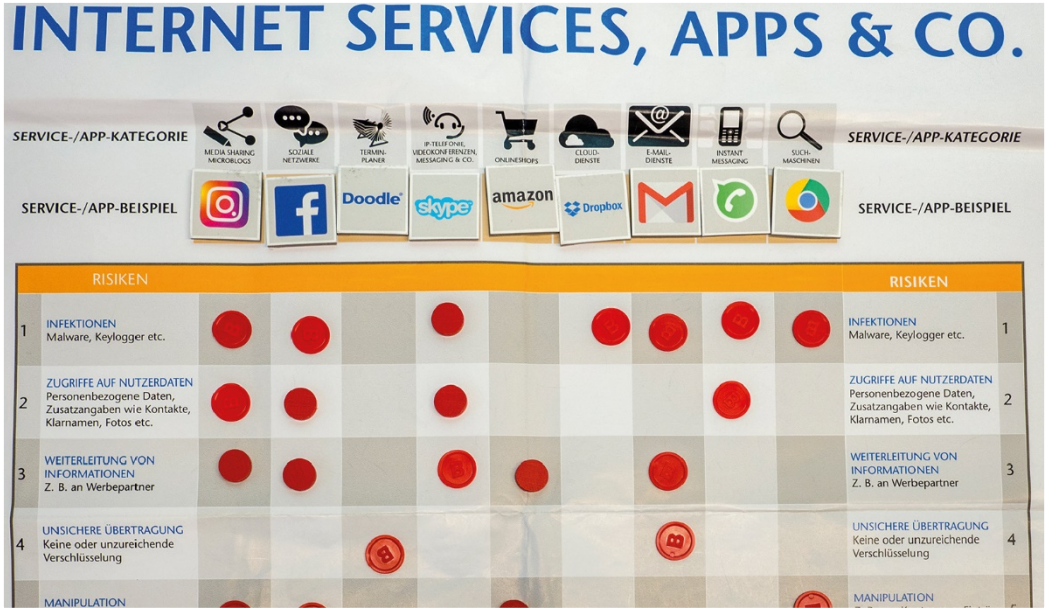


Fig. 143 Analog learning scenario "Internet Services, Apps & Co." for recognizing risks when using such services. The scenario is part of the "Security Arena" and is licensed by the company known_sense [39].

Fig. 144 Analog learning scenario as an aid to memorizing terms from all areas of IS, developed at TH Wildau with students in the "SecAware4job" project [45].

IT-Sicherheit 1 (Organisation)			
Hat Ihre *Leitung* Sicherheitsziele vorgegeben?	Wird bei Ihnen die Wirksamkeit von Sicherheitsmaßnahmen *regelmäßig* überprüft?	Ist in Ihrer Institution eine *Person* für Informationssicherheit zuständig?	Wird bei Ihr die Informationssicherh bei allen ne en Projekte *berücksichtigt*?
Wissen Sie,	Wissen Sie,	Werden neue	Sichern Sie

IT-Sicherheit 2 (Person)			
Können Sie „Spyware" *erklären*?	Können Sie den Grundwert „Integrität" *erklären*?	Aktualisieren Sie Ihr Virenschutzprogramm *täglich*?	Werden Dat mit https *ver schlüsselt* übertragen?
Wissen Sie, wie Sie sich bei *Brand* verhalten müssen?	Können Sie den Begriff „Authentifizierung" *erklären*?	Wissen Sie, warum *Essen und trinken* am PC unterbleiben soll?	Sichern Sie *regelmäßig* Ihre Daten?

Fig. 145 Analog learning scenario based on "Bingo" that can be used for exchanging information about the situation in an organization and for memorizing terms, developed by M. Scholl at TH Wildau, 2011.

Another idea that students came up with was for a serious game that could be used to help learners commit the different topics to memory (see fig. 144). Players need to guess the terms at the top of the card. The person describing the term is not allowed to use the expressions below it.

The last learning scenario shown in this chapter is one that was developed on the basis of the game Bingo, but adapted as a table containing questions about IS (fig. 145). The participants are divided into two groups. One group is given the sheet "IT security 1 (organization)" and the other, "IT security 2 (person)." The people in the two groups then ask each other questions. The names of the individuals being asked the questions are noted down. If, in one vertical, horizontal, or diagonal row of the question table, all the questions asked by the different people are answered "Yes," then "Bingo" can be called. The moderator then checks whether the answers are factually correct: the people whose names have been noted are asked for the specific definition of a term or for their answer to the question. If all the answers are correct and the "bingo" (of four questions) is fulfilled, then that participant has won.

Please test yourself using the following questions and comments for chapter 5.5:

- Explain how a router works.
- Explain when and why the use of a VPN connection is not just sensible but an absolute necessity.
- Explain the difference between "blacklist" and "whitelist."
- Explain the range of different tasks an ISO must carry out when implementing measures to establish secure networks in an institution.

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

5.6 Interesting facts about encryption and electronic signatures

Cryptology is the practice and study of techniques for securing information using mathematical processes. It has two subsections: *cryptography*, which includes the development of encryption methods and other security processes, and *cryptanalysis*, which examines the security of cryptographic methods and procedures. Cryptographic methods have become a key technology for IS in many applications. Knowledge of important terms and basic cryptography procedures is therefore essential for ISOs.

Cryptographic methods offer solutions to security problems that, in contrast to the TOM discussed so far, are of a *mathematical and logical nature*. In the case of cryptographic processes, an algorithm is implemented as a concrete technical measure. An algorithm is a defined computing process comprising rules for transforming data. It is used, for example, to turn original data that is readable/comprehensible into data that can no longer be read or understood. It is not absolutely necessary for an algorithm to be kept secret—it should rather be checked for vulnerabilities. The effectiveness of the cryptographic method is based on potential attackers being unable to solve a specific mathematical problem. Not because they lack the necessary skill but because they do not know very specific "key" information. The term *key* designates information used for data transformations. The original data cannot be restored without knowledge of the key [118]. The security depends on the quality of the keys used and on their secure handling. Nowadays, keys are bit numbers of various lengths. The security therefore depends on the key length. Procedures are considered to be *secure in practical terms* if attackers cannot conceivably break the encryption in real time either on their own or with the help of high-performance state-of-the-art computers. Theoretically, any encryption can be broken, if necessary by trying out every possible key—this is called a *brute force attack* [1].

There are two different types of encryption methods: *symmetric* and *asymmetric* encryption. Since both methods have advantages and disadvantages, a combination has been developed—*hybrid* encryption—that harnesses the advantages of both methods and is often be used for secure hypertext protocol *https*. The asymmetric encryption procedure also makes *digital signatures* possible.

The goals of cryptographic protection are [1]:

- confidentiality through encryption processes,
- integrity through hash procedures or MACs (Message Authentication Codes),
- authenticity and liability through electronic signatures and cryptographic protocols.

It should be noted that encryption does not protect against attacks on the availability of data and applications.

The *symmetric* encryption procedure is also called the *private key procedure*, because it is identified by a single key. This key S_{sym} encrypts the original data on the sender side and decrypts the encrypted data again on the recipient side. The best-known symmetric key algorithm currently recommended by the BSI is the Advanced Encryption Standard (AES) with key lengths of 128, 196, or 256 bits [118]. The following advantages and disadvantages are associated with symmetric methods:

- The advantage is that these algorithms work very quickly and are thus suitable for encrypting large amounts of data.
- The first disadvantage is that this key has to be transmitted from the sender to the recipient on a transmission channel that is confidential and different from that used for the transmission of the data.
- The second disadvantage is complex key management, because the greater the number of people taking part in an encrypted exchange of messages, the more separate symmetric keys are required and the greater the risk that a symmetric key will become known in the event of carelessness.

The *asymmetric* encryption procedure, which is also called the *public key procedure*, is therefore based on a different idea: a key pair is generated that consists of a public key S_{public} and a private key $S_{private}$. The public key is made available, for example, by accredited providers on key servers. The user must keep their individual private key secret. It is important that the mathematical functions used in the generation of key pairs ensure that it is impossible *in practical terms* to derive the appropriate private key from the publicly available key. For the application, it is important to note that the recipient's public key $S_{Rpublic}$ must always be encrypted so that the recipient can decrypt it again with his private key $S_{Rprivate}$.

The best-known asymmetric key algorithm is probably the method authored by Rivest, Shamir, and Adleman (RSA). Up to the end of 2022, the BSI requires a key length of at least 2,000 bits for it to be used effectively, and after that at least 3,000 bits. The following advantages and disadvantages are associated with asymmetric procedures [1]:

- One disadvantage is that these algorithms work much slower than symmetric ones and are therefore less suitable for encrypting large amounts of data.
- There are much better methods of attack, so the key pair generation is more complex, and the key lengths must be much longer.
- In addition, a public key infrastructure must be set up to ensure that a public key actually belongs to a specific person.
- The users must secure their private key in order to make it more difficult for attackers to misuse it.
- The advantage of the asymmetric procedure is that the key management is much simpler.

Hybrid encryption combines the advantages of symmetric and asymmetric encryption and, as already mentioned, is the basis for protecting the protocol http with Secure Sockets Layer (SSL) or Transport Layer Security (TLS), resulting in https. The rough procedure is as follows:

- A symmetric session key S_{sym} is created via a random process, with which plain text or large amounts of data can be encrypted.
- This session key S_{sym} is encrypted (using the asymmetric procedure) with the public key of the recipient $S_{Rpublic}$ and sent over the network. There it can be decrypted with the private key of the recipient $S_{Rprivate}$. Afterwards, the symmetric key for encrypting the data is available on both sides.
- The data is symmetrically encrypted on both sides (sender, recipient, and vice versa), sent over the network and decrypted again on the other side with S_{sym}.

The *digital signature* is not primarily about the encryption of a plain text, such as a contract, but the electronic equivalent of a personal signature. Electronic signatures combine asymmetric cryptographic algorithms with procedures for securing integrity, the cryptographic hash functions [1]. Hash functions generate a hash value from any character string with the following properties:

- The hash value cannot easily be used to infer the original character string.
- It is impossible *in practical terms* to form two different character strings that produce the same hash value.

The Secure Hash Algorithm (SHA) family is an example of the most frequently used cryptographic hash functions. The BSI recommends the use of the hash functions of the SHA-2 or SHA-3 family, which generate hash values with a length of 256, 384, or 512 bits [119].

For the user, this means in practice that a certain document receives a unique hash value. For this, the private key of the sender $S_{Sprivate}$ can be used in the asymmetric procedure. The application of $S_{Sprivate}$ to the data—i.e., the digital signature—causes the hash value to be encrypted. In simple terms, this electronic signature is the encryption of the hash value of the signed document. If the document signed by the sender arrives electronically on the recipient side, the sender's signature can be checked there with the sender's public key $S_{Spublic}$. If the check is positive, the hash value of the document could be decrypted, and it is clear that this value was encrypted with the private key of the sender. If the hash value of the document is generated again on the recipient side, and if this is identical to the decrypted hash value, the *integrity* is confirmed: no data manipulation took place on the way via the Internet.

The authenticity of the sender is clearly given if the procedure is carried out via a certification authority with a corresponding public key infrastructure. The certification authority uses its own private key to add a signature to data belonging to the sender and thus to generate a digital certificate. Many applications check the validity of digital certificates.

The format of a certificate, which corresponds to the international standard X.509, contains the following information [1]:

- X.509 version used (currently version 3)
- serial number of the certificate
- identification of the algorithm used for the signature
- name of the certification authority and the validity (start, end)
- name of the certificate owner (name, organization, etc.)
- algorithm identifier and public key of the certificate holder
- purpose of the public key / encryption or signature verification
- X.509 extensions (to identify the certificate owner, information on key usage, certificate checking service, etc.)
- algorithm identifier and signature of the certification authority.

Implementation and training exercises to raise awareness of IS

For millennia, encryption techniques have been used to keep messages secret: these techniques have been of great importance, and no less significant has been the urge to unravel their secrets. This chapter can thus be enriched with a look at the historical background and the facts associated with it. An early example of an idea of symmetric analog encryption is the *Skytale of Sparta*. Strips of writable materials were wrapped around cylinders of different diameters and the sender wrote on them transversely. Once processed, a carrier was able to deliver the sender's (incomprehensible) strips to the recipient. The recipient was able to read the strips using a previously agreed diameter of the cylinder. Another recent example is the decryption of the complicated German encryption machine Enigma during World War II. Its ability to decrypt messages is thought to have given the Allies a crucial advantage, which led to Germany's surrender and thus significantly shortened the war. We recommend the book *The Code Book* (in German: *Geheime Botschaften*) by Simon Singh [120], which gives an account of the art of encryption from antiquity to the days of the Internet.

In addition, there are many videos on this topic on the World Wide Web, which, depending on the target group and the design of the training, can be used to illustrate encryption procedures. In the following, we will explain our ideas for the exercise, starting with the simplest encryption and decryption based on the Caesar cipher. This is followed by a software-based exercise on email encryption and advanced digital signatures. At the end, we briefly cover the development of a crypto concept.

Julius Caesar is said to have used a simple (and insecure) symmetric encryption method (fig. 146), which is based on monographic and mono-alphabetic substitution: shift the alphabet of the plain text by, for example, four digits to the right and you get the alphabet for the cipher text. If the recipient side knows the number of shifts, it can decode the cipher text. Such simple procedures can be broken by statistical analyses of the frequency of individual characters or character strings and are completely inadequate today. Because of its simplicity, however, this cipher can be used for a memorable illustration of the basic principles of cryptology.

Plaintext alphabet:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
Chipher text alphabet:
DEFGHIJKLMNOPQRSTUVWXYZABC

Fig. 146 Principle of the Caesar cipher.

In the *Security* project, the following learning scenario was developed with the aim of providing students with a basic knowledge of encryption and its possible uses, as well as haptic testing. The aim is to prompt an awareness of the importance of encryption. In the first phase, assigning the terms available for selection initiates an exchange about students' personal knowledge of the topic (fig. 147, above). After that, the moderator of the learning scenario can deal more specifically with the processes of cryptography and cryptanalysis (fig. 147, bottom).

Fig. 147 Raising awareness of cryptographic basics. Here: the game playing field (phase 1), developed in German as part of the "Security" project [50]. Schools can borrow the learning scenario from the project website [46].

The second phase focuses on giving encryption and decryption at try. For this purpose, we have acquired secret boxes known as “Da Vinci boxes” (see fig. 148). These are configured with a password, which can be discovered as part of an exercise using a story about the Caesar cipher. The story involves three emails being distributed to the participants providing information about the alphabetic shift. The story can easily be adapted to the age of the target audience. A prepared sheet of paper with the German alphabet is also distributed on which the participants can enter the shifts they have identified. If the participants are young pupils, an explanatory sheet on the Caesar cipher can also be handed out as a reminder. The aim is to recognize the password of the secret box individually or as a group in a competition. The winner is the person or team who can open the secret box first.

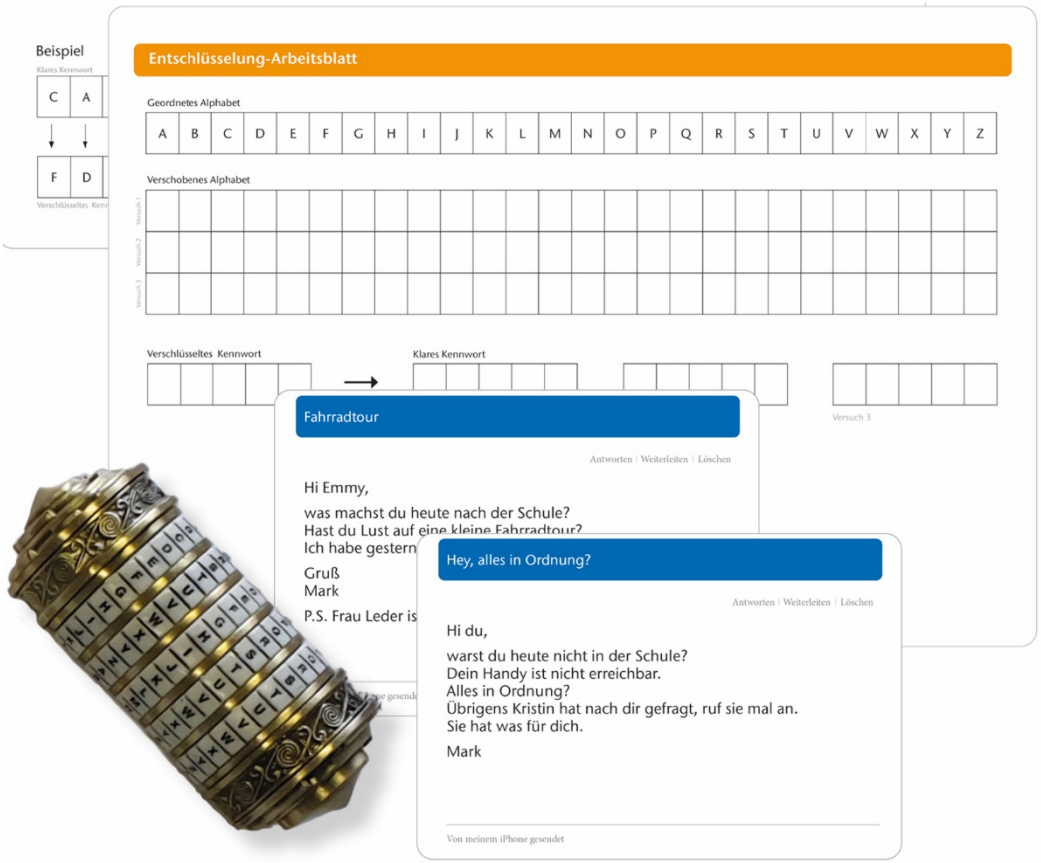


Fig. 148 Raising awareness of cryptographic principles using the Caesar cipher. Here: phase 2, developed in German as part of the “Security” project [50] and available for schools to borrow via the project website [46]

Encryption of confidential data is useful—for example, when using hard drives in insecure environments. In addition, the GDPR refers in general (see chapter 5.4)—and, in particular, in Article 32—to the encryption of personal data as a protective measure. There are different software and hardware options for hard disk and file encryption, which typically use symmetric methods. When deciding which encryption product to choose in practice, the data protection requirements must be assumed.

As a second exercise, we will explore the asymmetric method. We want to use software to clarify the principles of modern encryption in an easy way. The exercise can be expanded to illustrate the digital signature. In relation to German signature law, such a signature used internally would be a so-called advanced, rather than a qualified signature. The latter needs a certification authority. In this exercise, we show the encryption between two mail clients using open-source software (see, for example, [121] and [122]). For this exercise, we use the functions of the software but configure as many things as possible manually in order to get a better understanding of the process. We use two mail clients as a basis (Mozilla Thunderbird version 68.8.1 including the Enigmail add-on). In addition, the gpg4win software version 3.1.11 was installed on each client system. The exercise also makes use of two mail accounts: mailer1@wildau.biz and mailer2@wildau.biz.

1. In the first step, a key pair must be created on each client for the asymmetric procedure. To do this, start the Kleopatra key management software supplied with gpg4win and click on the “new key pair” button (fig. 149—in German: “Neues Schlüsselpaar”). If the preset automatic software has already created a key during installation, please delete it.

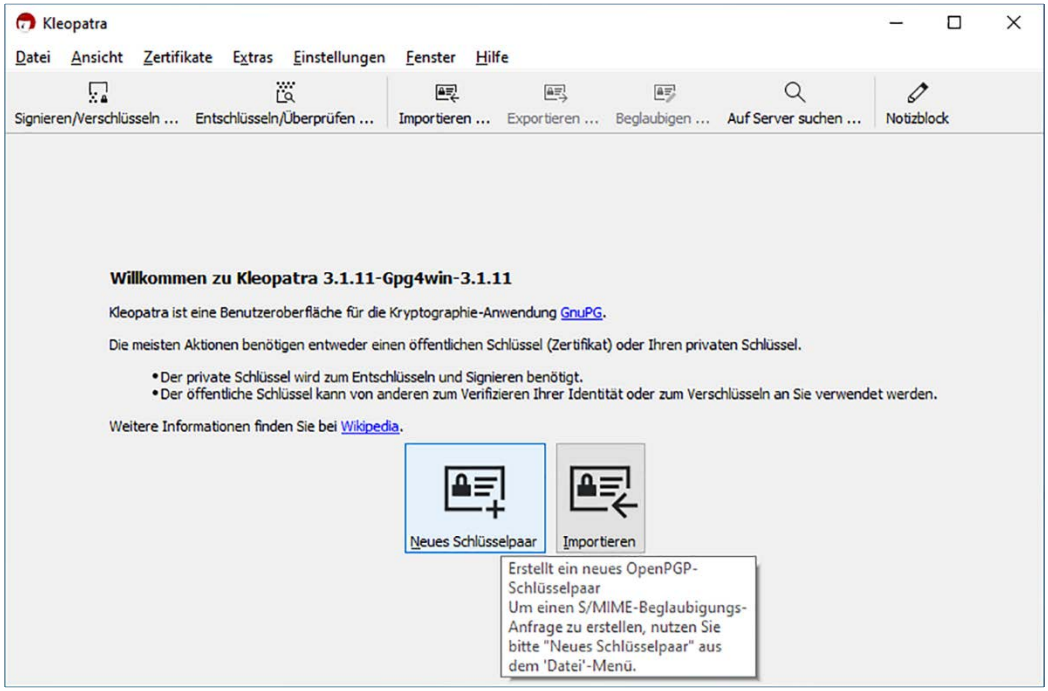


Fig. 149 The key management software “Kleopatra” after the initial start is used to generate a new key pair for the asymmetric encryption process.

2. A name and an email address must be entered. Please make sure that these are correct. As can be seen in fig. 150, enter the data mailer1@wildau.biz and mailer2@wildau.biz on the respective client. Click on “Next” (in German: “Weiter”) and then on “Create” (in German: “Erstellen”).

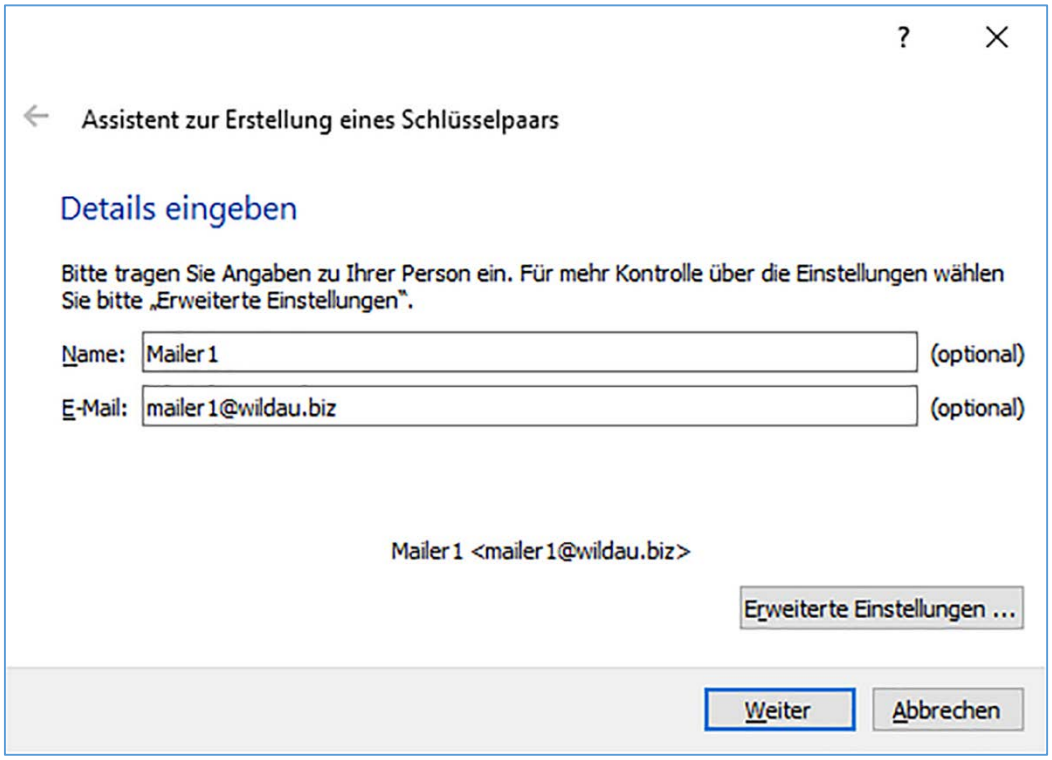


Fig. 150 Data input for both mail clients. Here, for mail client 1, the name is Mailer1 and the email address is mailer1@wildau.biz.

3. You must secure the private part of the key pair with a password (see fig. 151). Make sure that your chosen password is secure and that you can remember it. It is not possible to change the password afterwards or to reset it! Confirm the entry with "OK."

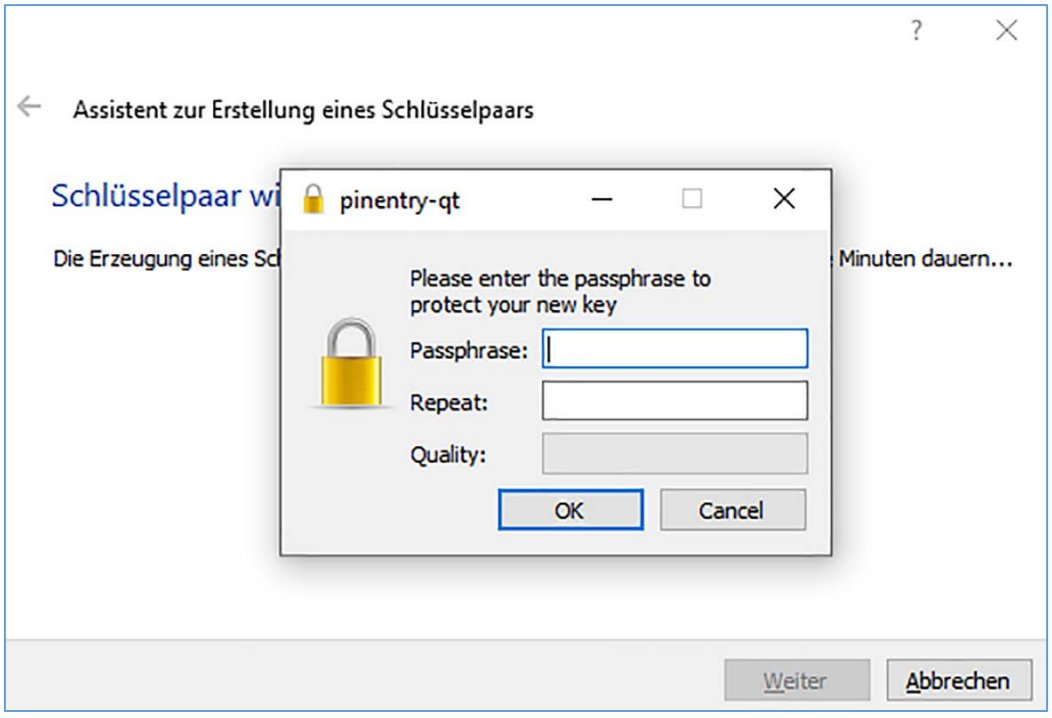


Fig. 151 Password input for the private key of the key pair.

4. After successful key generation, you will see a different fingerprint for each of the two mail clients on the screen (fig. 152). Click on “Finish” (in German: “Abschließen”).

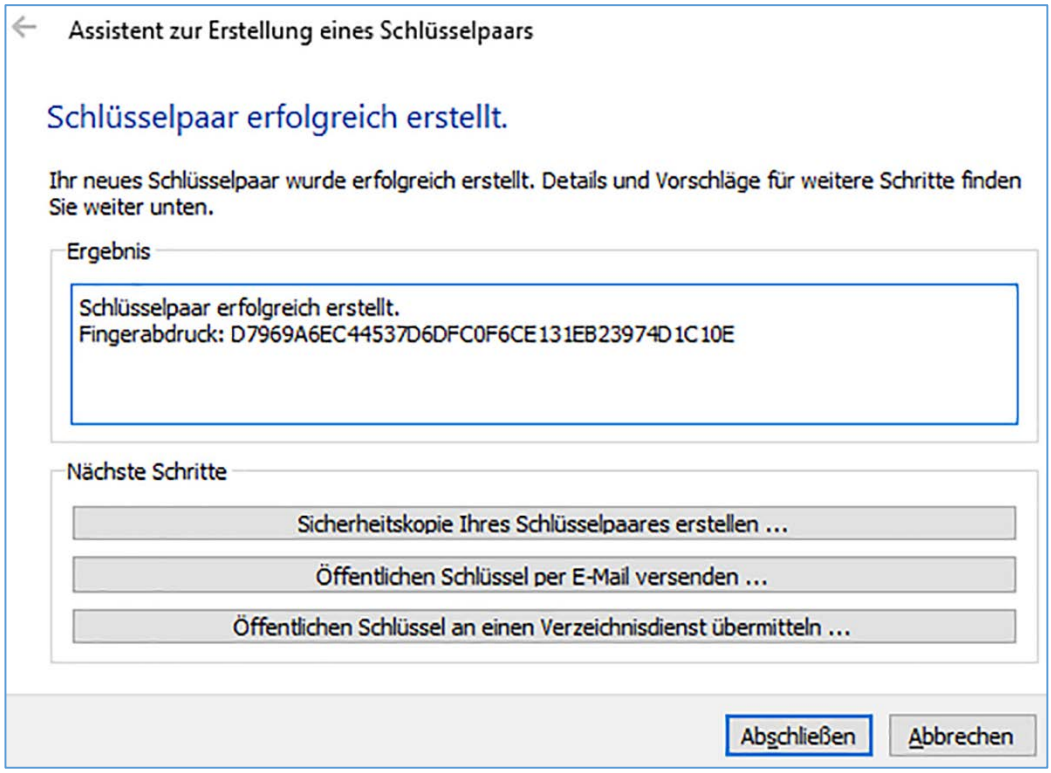


Fig. 152 A key pair has been created successfully.

5. In the next step, the respective counterpart is provided with the public part of the recipient’s key (fig. 153). To do this, this part is exported from Kleopatra: right-click on your public key (in fig. 153 for Mailer1) and select the option “Export” (in German: “Exportieren”).

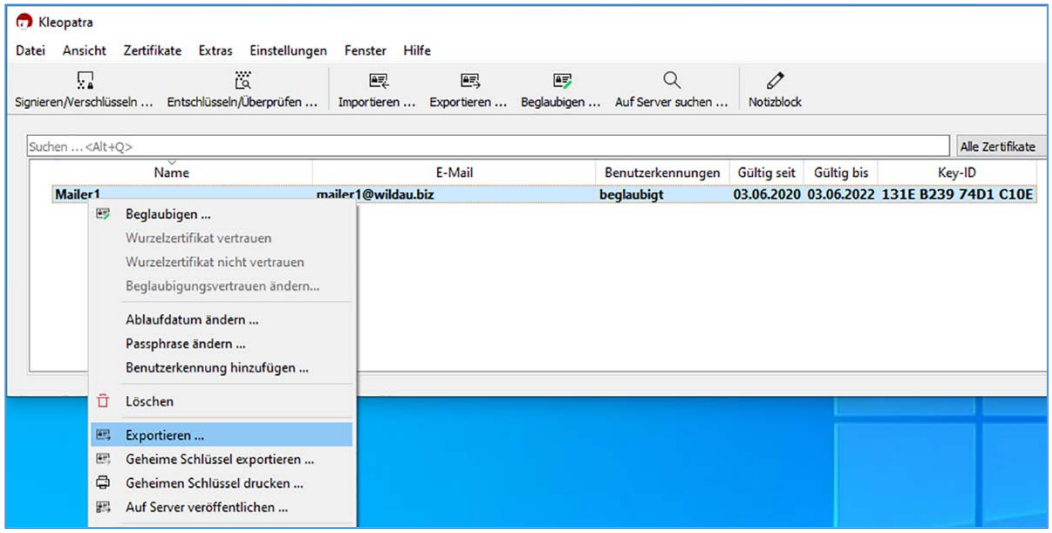


Fig. 153 Export of a public key in the “Kleopatra” tool.

6. Export your individual public key to your client's desktop and name it so that it is easy to recognize—e.g., Mailer1public (see fig. 154, in German: Mailer1öffentlich).

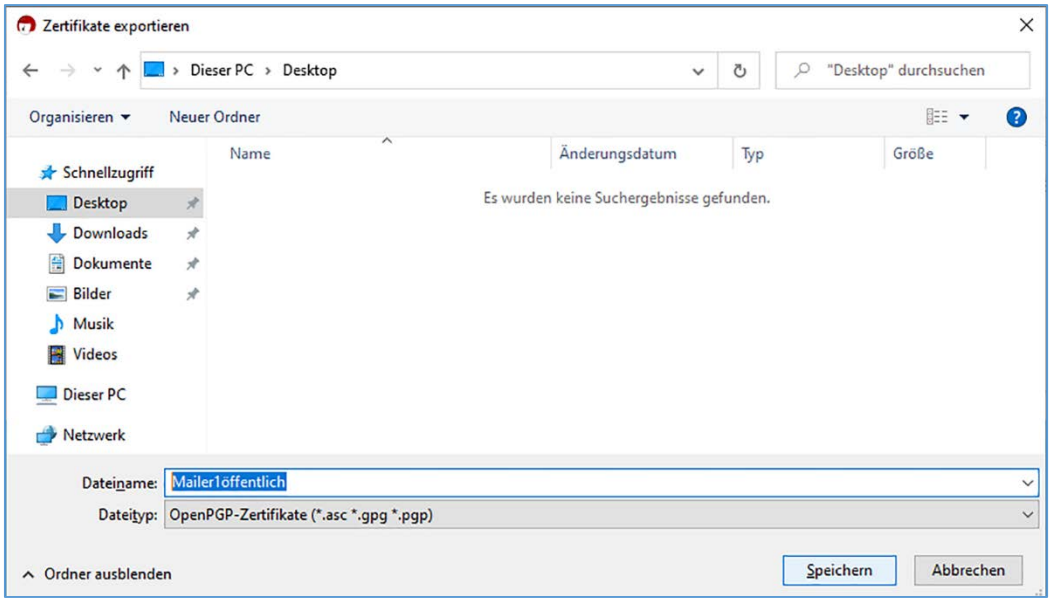


Fig. 154 Save your own public key (e.g., on the desktop of the PC).

7. These two public keys must be exchanged between the two clients. For the exercise, the other person's public key is copied to your own desktop as a personal transfer.

   At this point, it becomes clear why an official certification authority must use a Public Key Infrastructure (PKI) on the Internet to ensure that the public key really belongs to the relevant person.

8. Drag & drop the public key of your counterpart into the *Kleopatra* tool and select "Import Certificates" (fig. 155, in German: "Zertifikate importieren").

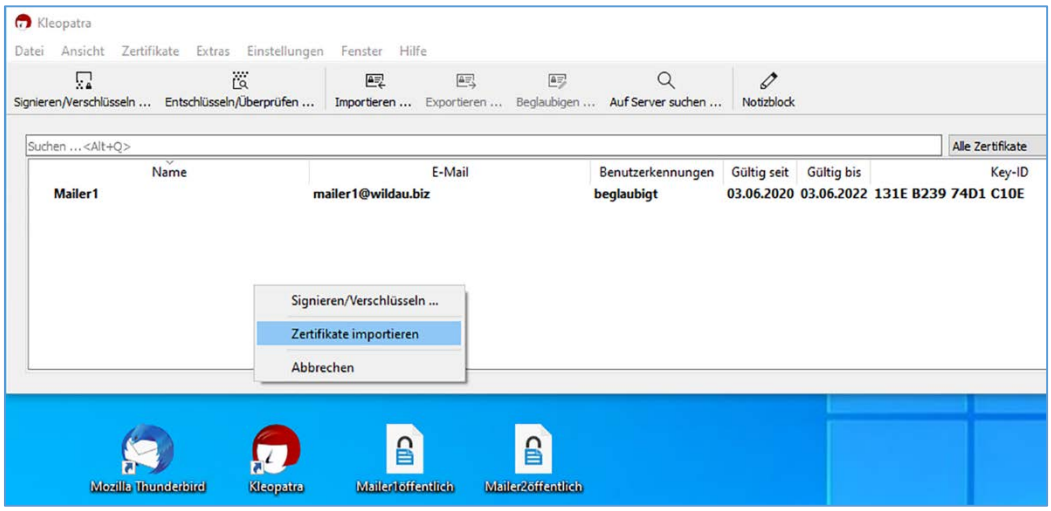


Fig. 155 Initial situation of client 1 (Mailer1) and first step of importing the public key from Mailer 2.

9. The Kleopatra tool checks the public key to be imported and reminds you to secure the identity of the issuer (fig. 156). After clicking on “Yes” (in German: “Ja”) and “Authenticate” (in German: “Beglaubigen”) on the following screen, the tool will authenticate/sign the public key of your counterpart (in the example, Mailer2) with your own private key (in the example, Mailer1) and store the public key in the key chain (figs. 157 and 158). For authentication, you will have to enter the password of your private, password-protected key in the final step (fig. 158).

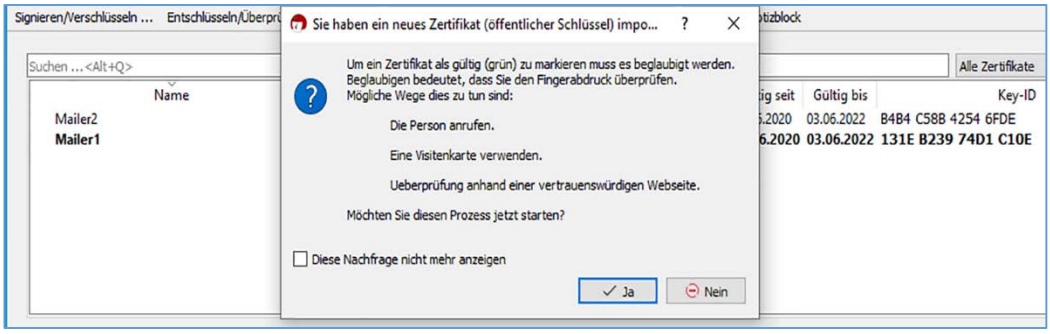


Fig. 156 Situation of client 1 (Mailer1) and the second step of the import of the public key from Mailer2 in the “Kleopatra” tool: information from the tool for authentication of the public key.

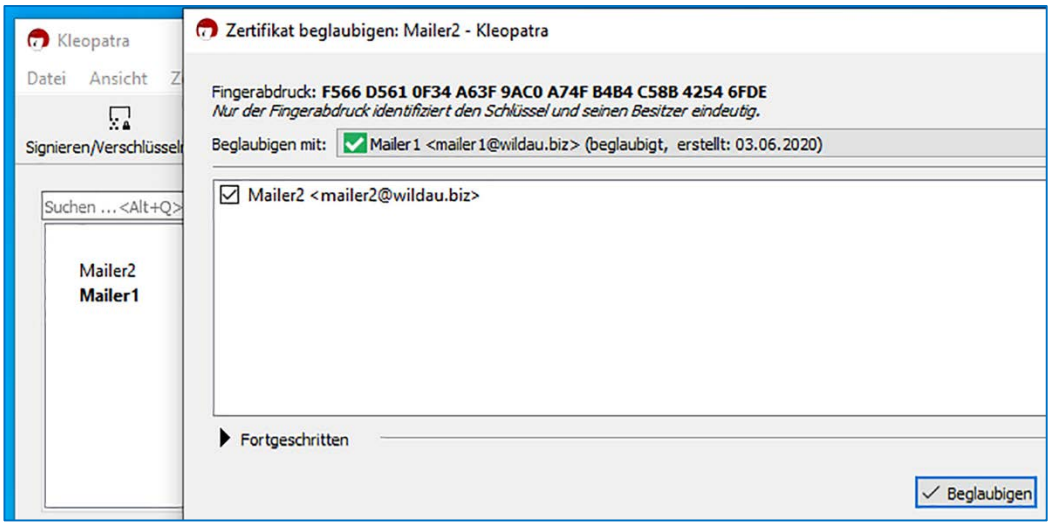


Fig. 157 Situation of client 1 (Mailer1) and the third step of the import of the public key of Mailer2: authentication of the public key of Mailer2 with the private key of Mailer1.

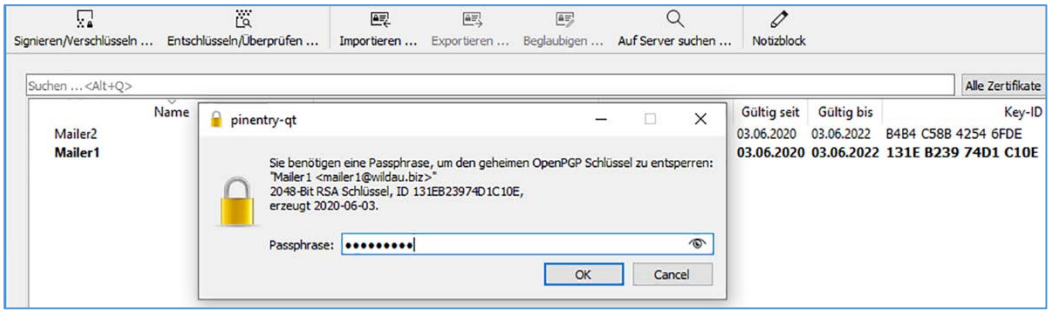


Fig. 158 Situation of client 1 (Mailer1) and the fourth step in the import of the public key of Mailer2: confirmation of the public key of Mailer2 with the private key of Mailer1 by entering the password from Mailer1.

10. The situation achieved between the two mail clients can be seen in the two figures below. Your own key pair is shown in bold in the *Kleopatra* tool and the public key of your counterpart can also be seen in your key chain. Fig. 159 illustrates the situation from the perspective of the first mail client, and fig. 160 shows it from the perspective of the second mail client. Compare the two screenshots from the key management of Mailer1 and Mailer2. Note the fingerprint in the last column.
    The necessary keys are now available on both sides allowing learners to practice encrypted email traffic with one another.

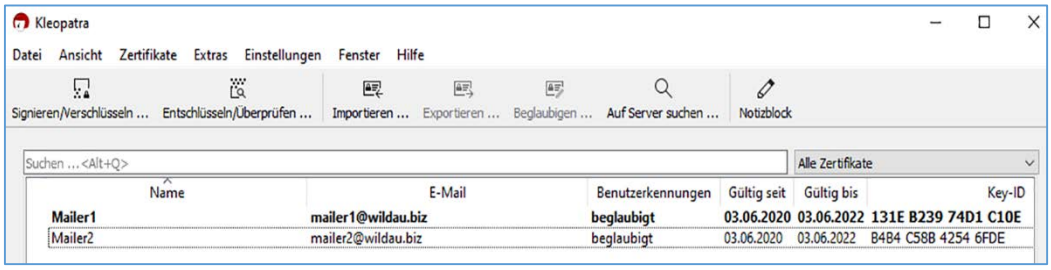


Fig. 159 Keys from the perspective of Mailer1.

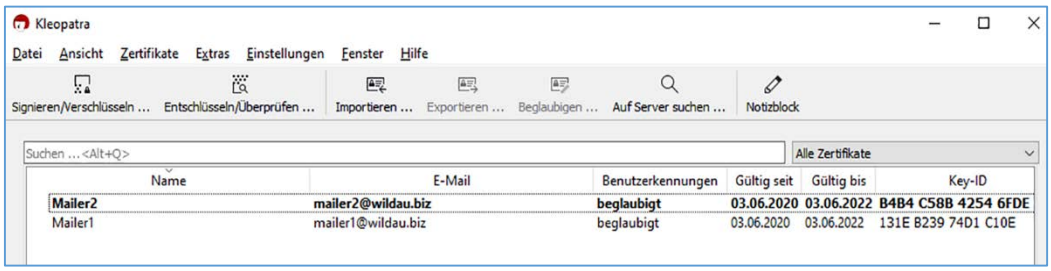


Fig. 160 Keys from the perspective of Mailer2.

11. Close the *Kleopatra* tool and start *Mozilla Thunderbird*. Switch to the “Account Settings” (in German: “Konten-Einstellungen”) via the “Extras” menu item (fig. 161).

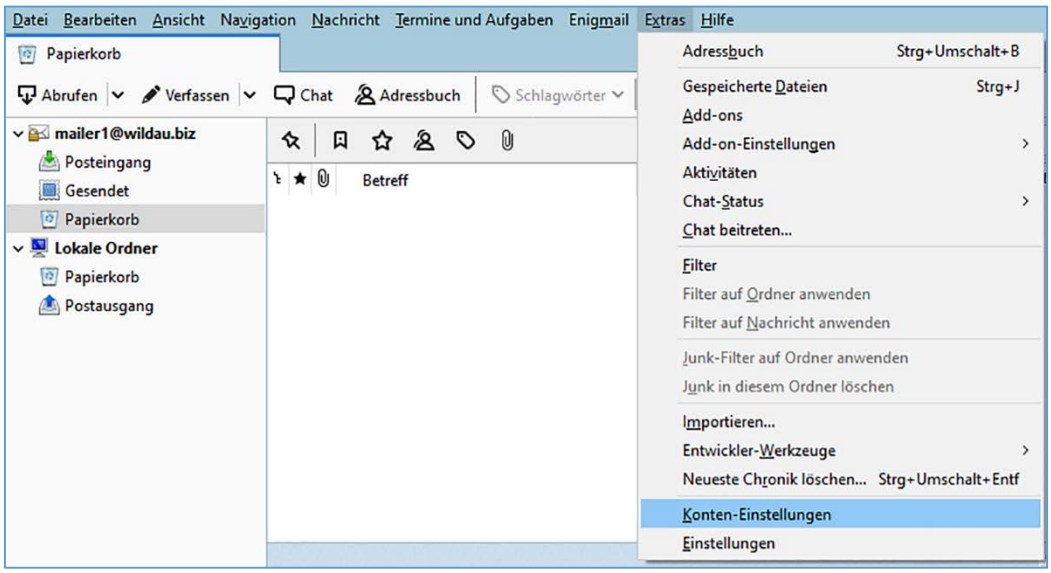


Fig. 161 Account settings in Mozilla Thunderbird.

12. In Mozilla Thunderbird's "Account Settings," select the "OpenPGP Security" settings (see fig. 162). Set the options as shown in the following figure and confirm the changes with "OK."

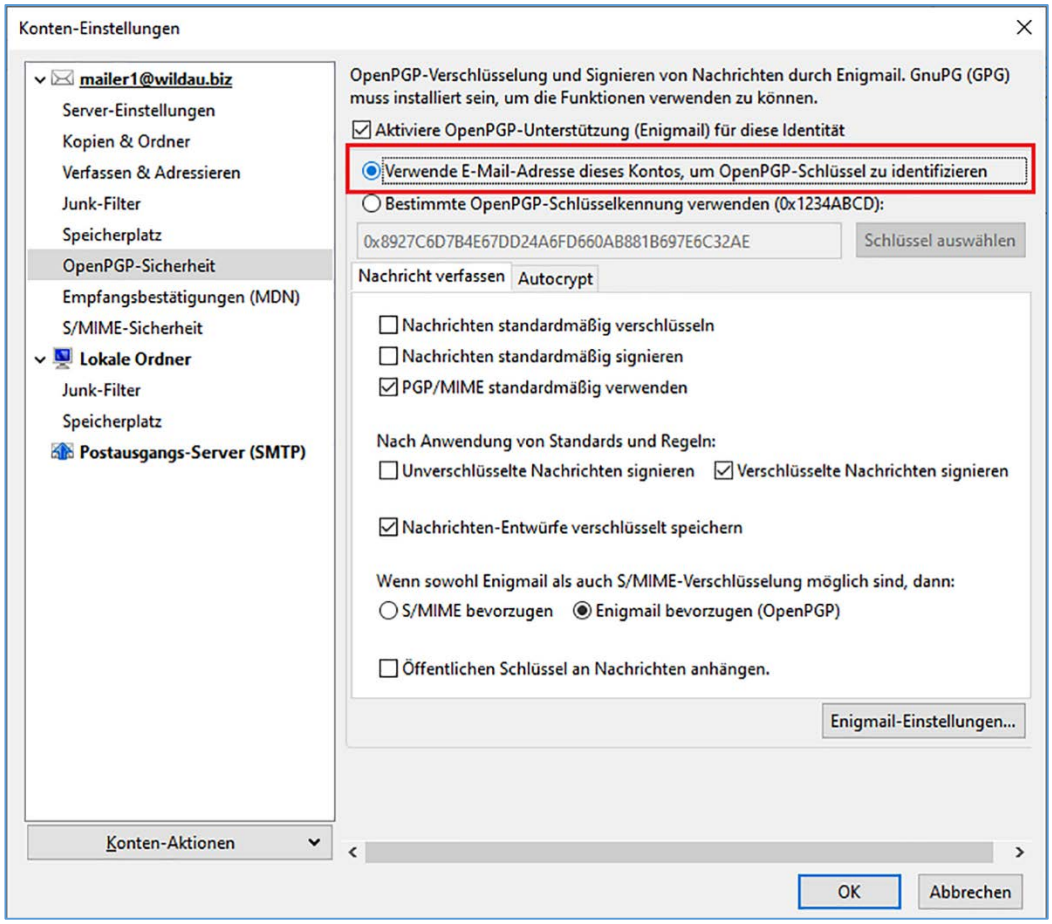


Fig. 162 Options for "OpenPGP security" in the "Account Settings" of Mozilla Thunderbird.

Once the two clients have been successfully configured and the public keys of the two counterparts have been exchanged and authenticated, these clients can now exchange encrypted and signed mails with one another. In the next steps of the exercise, we will take a closer look at the encryption of emails.

13. As Mailer1, write a small text, encrypt it with the correct key, and send it in encrypted form to Mailer2 (fig. 163).

14. When you receive the message as Mailer2, there is very little to see at first, as Mailer2's public key was used for encryption. For decryption you need the private key of Mailer2 and the password of this protected key (fig. 164).

15. After entering the password, the message is completely legible for Mailer2 (fig. 165).

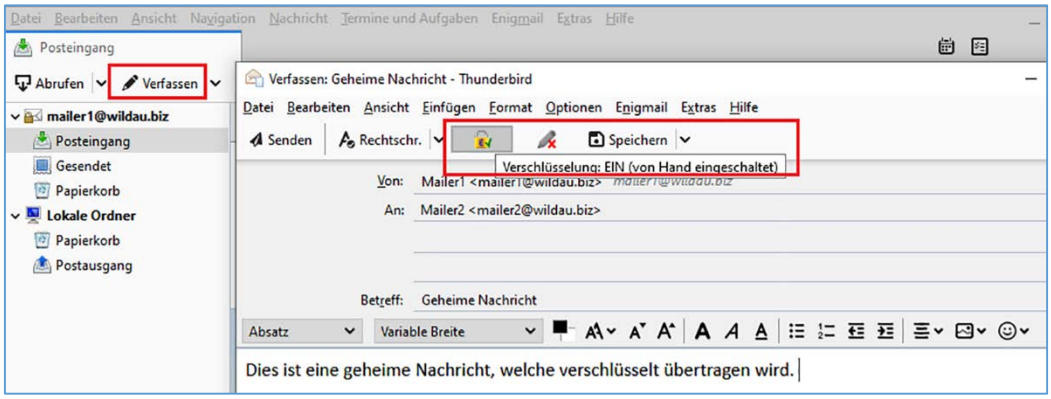


Fig. 163 Composition of an encrypted but unsigned message sent from "Mailer1" to "Mailer2".

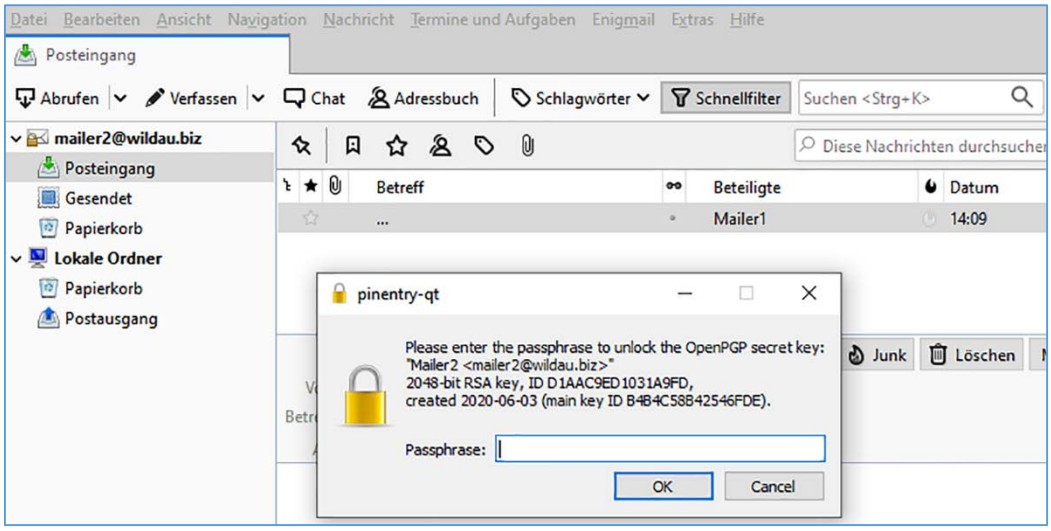


Fig. 164 Receipt of the message and request for the password for the protected private key of "Mailer2".

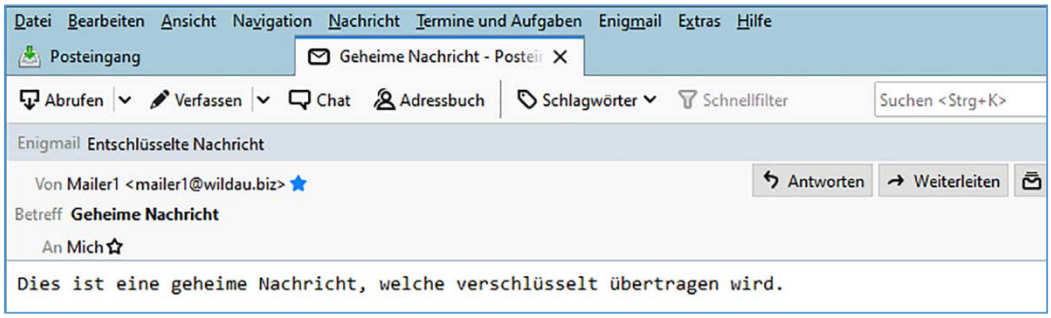


Fig. 165 The message to "Mailer2" was successfully decrypted by "Mailer2" with the private key and can now be read.

16. After opening the message, press the key combination "Ctrl + U" to see the source text of the message (fig. 166). In addition to a variety of *header information*, there are three elements that are relevant to us in the upper part of the message: first of all, the recipient name and account are displayed here with "To." "From" shows this for the sender side. The *public key* of the sender side is then written by the software using "Autocrypt."

Fig. 166 The message header automatically generated by the software.

The public key is named automatically in the software, regardless of whether the message was encrypted or signed. The public key of the sender side is always automatically written into the header information of every email sent. In this way, the public key can be distributed and compared if there are any deviations.

17. The actual encrypted message begins in the lower third of the source text of the message (fig. 167).

    First, the temporary subject is defined with “Subject: …,” which is displayed until you are able to decrypt the message.
    Then, in addition to further header information, there is also an indication that the message has been encrypted, with the type of encryption specified. You can also see that the encryption is highlighted and bounded by the following marker:
    boundary = “8Y55oSr3MzVBGJRx11HjGrtw1kbHMrLUS.”
    The actual encrypted message including the subject is between “BEGIN PGP MESSAGE” and “END PGP MESSAGE.” It is actually sent as an encrypted file “encrypted.asc”—i.e., as a mail attachment.
    Select the contents of the encrypted file as shown in the following figure. Copy this into the clipboard by right-clicking on the marked text and “Copy” (fig. 167, in German: “Kopieren”).

Fig. 167 Further source text of the encrypted message sent to "Mailer2".

18. Start the *Kleopatra* tool again and select the "Clipboard" (in German: "Zwischenablage") under "Extras" and the "Decrypt/Check" option (fig. 168, in German: "Entschlüsseln/Überprüfen").

19. The *Kleopatra* tool will then ask you again for the password of your private key in order to be able to use it. After entering the password and confirming it, you should receive the message shown in fig. 169.

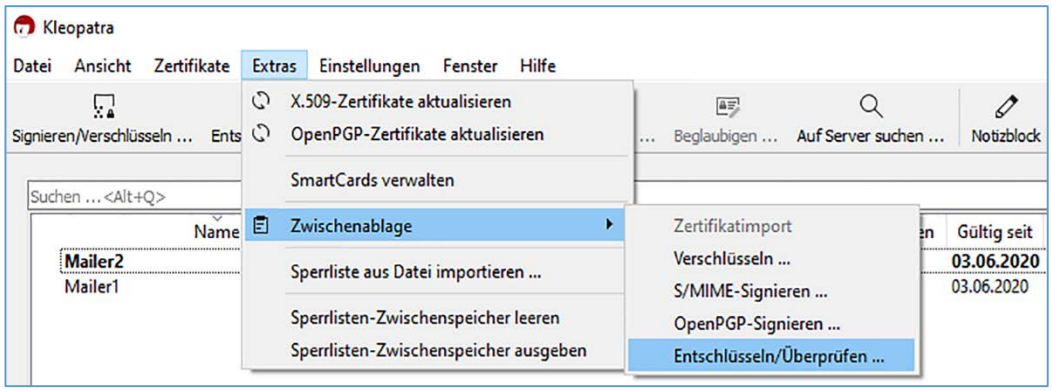


Fig. 168 Manual decryption option of the message sent to "Mailer2" in the "Kleopatra" tool.

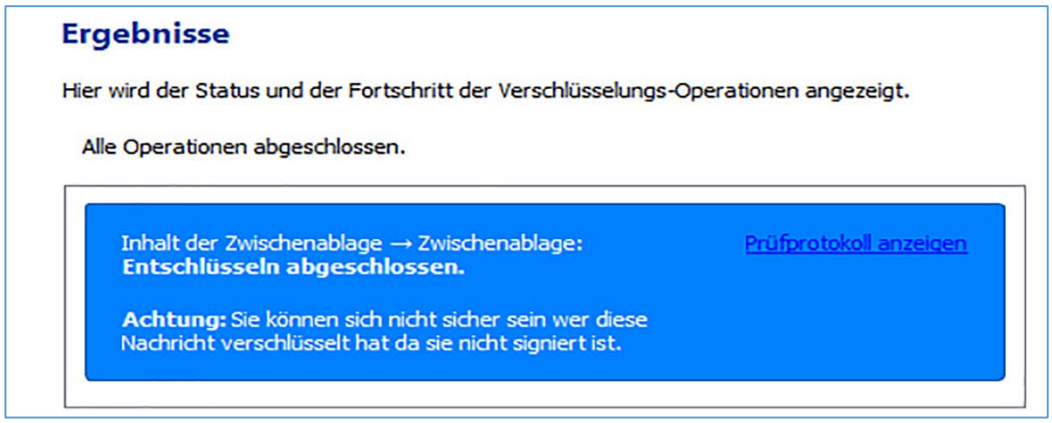


Fig. 169 Confirmation of the manual decryption in the "Kleopatra" tool.

20. You have decrypted the message on your clipboard. Open any word processor or editor. Paste the decrypted contents of the clipboard into the editor. You should be able to read the original mail including the subject "Secret Message" (fig. 170).

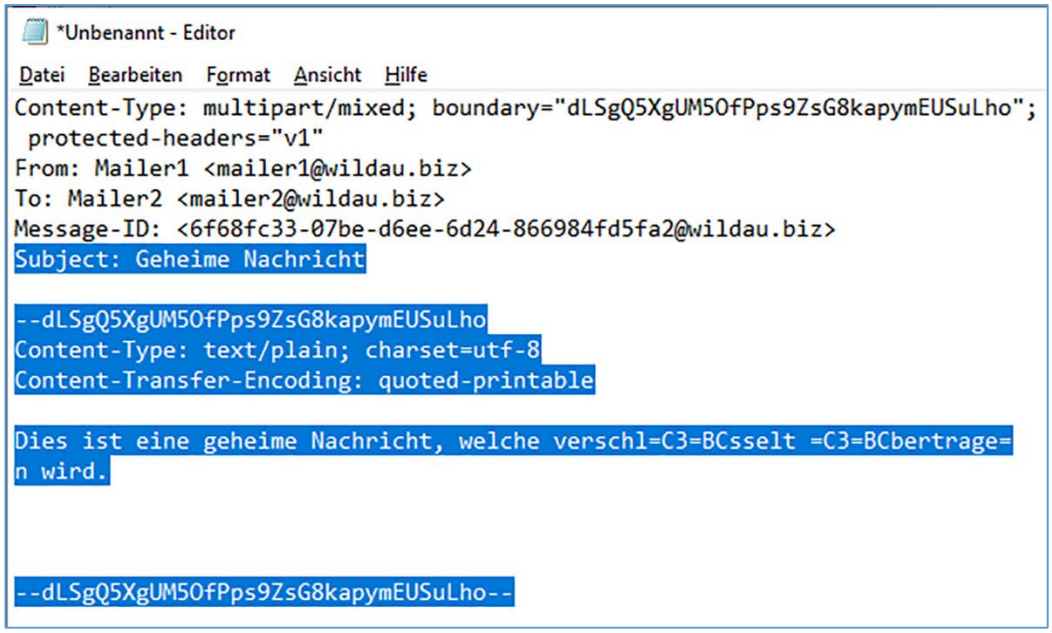


Fig. 170 Source text of the manually decrypted message sent to "Mailer2".

The tool-based exercise on encryption in the asymmetric procedure is now complete. The third awareness-raising exercise in chapter 5.6 relates to an organization's crypto concept.

The development of a crypto concept is to be integrated into the information security concept of an institution according to fig. 1 after careful analysis of the specific circumstances. It is a part of the security concept and cannot replace it. It documents the areas of application in the institution where cryptographic protection mechanisms are required and indicates which processes and products are used and which organizational rules and precautions apply. Often, however, it is not clear to ISOs how the institution's crypto concept document should be structured. The BSI's 2008 guideline for creating crypto concepts provides information on this, including annexes [123]. The BSI's sample crypto concept from 2010 [124] can also be used.

Our final exercise in chapter 5.6 revolves around the sample structure of a crypto concept. The most important points from [124] are printed out on separate sheets and should be exchanged and compiled by participants in order to create an outline structure (fig. 171). The exchange of information about what term has what meaning in what context promotes understanding of how such a document could potentially be structured—"potentially," because every institution has specific cryptographic conditions and often has to observe individual specifications with regard to the written documentation. This exercise also makes it much clearer to all participants how much work is involved in creating this kind of crypto concept. At the end, the structure produced by the group can be compared with the original described in [124].

Fig. 171 Raising awareness about developing a crypto concept. Here: a collection of ideas for the structure of the document from participants in the training.

Please test yourself using the following questions and comments for chapter 5.6:

- Note the advantages and disadvantages of a symmetric encryption method.

- Note the advantages and disadvantages of an asymmetric encryption method.

- Explain the hybrid process using your online banking.

- You want to send Jane Doe an encrypted message using the asymmetric method. What key do you need to use for encryption? What key does Jane Doe need to use for decryption?

- You want to send John Doe a signed message using the asymmetric method. What key do you need to use for signing? What key does John Doe use and what are the consequences of this?

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

6 Ideas for business continuity management based on BSI Standard 100-4

We conclude this book by returning to the beginning. According to fig. 1 and table 1, business continuity management and the handling of security incidents must be set up parallel to the ISMS. In our opinion, BSI Standard 100-4 [125], which is currently being revised, offers crucial information for facilitating cooperation between BCOs and ISOs. It should be noted that BSI Standard 100-4 describes an independent management system for business continuity and emergency response. This pursues a different goal than that of the ISMS according to BSI Standards 200-1 to 200-3. The aim of BSI Standard 100-4 is to "show a systematic way of responding quickly to emergencies and crises of various types and origins that can lead to an interruption of business. It describes more than IT emergency management (IT service continuity management) and is therefore not to be seen as a sub-area of the ISMS." [125].

At the beginning, it is necessary to clarify the terms: What is the difference between the terms "disruption," "emergency," "crisis," and "disaster"? In short, a disruption is associated with a low level of damage and is generally remedied within the institution in the course of day-to-day business. The emergency is characterized by the fact that existing service level agreements (SLAs) cannot be adhered to and normal business operations cannot be maintained. High to very high levels of damage occur [125]. The ability of an institution to perform certain tasks is thus severely impaired, and emergencies can no longer be dealt with in the course of general day-to-day business. Contingency plans are thus required that should be defined and tested beforehand. In addition, separate emergency management organization is necessary [125]. Emergencies can escalate into a crisis. Crises can, however, also arise for the institution independently. The difference between emergencies and crises for an institution is that there are no operating plans for a crisis, which is always unique to some extent. A "crisis team" with decision-making authority is necessary. A crisis endangers the existence of the institution and possibly also people's life and health. Ultimately, however, the crisis still has to be overcome within the framework of the institution's business activities. A disaster, meanwhile, according to the BSI definition, cannot be remedied exclusively by the institution itself. Owing to its geographical spread and impact on the population, disaster protection is required, which in Germany is the task of the federal states and is supported by the federal government [125]. Each institution should therefore specifically define these four terms and the term "normal operation." For this purpose, we will present an idea for an exercise.

Before an emergency management system can be established in an organization, the framework conditions must first be clarified in accordance with BSI Standard 100-4 [125]. A guideline for business continuity management must be drawn up and initiated, co-developed, and approved at executive level (see fig. 1 and table 1). In addition, the organizational requirements and the budget for emergency management must be clarified.

"For business continuity management to succeed, it must be properly integrated at the conceptual level into the existing authority or corporate culture. For this purpose, the employees must be included in the process and prepared for their roles through awareness-raising and training measures" [125].

According to BSI Standard 100-4, the process is as follows [125]:

- Initiation of emergency and business continuity management
- Draft concept
- Implementation of the contingency planning concept
- Emergency response
- Tests and exercises
- Maintenance and continuous improvement of the business continuity management system (BCMS)

Here, two sides are clearly evident: contingency planning and emergency preparedness on the proactive side, and contingency management and emergency response on the reactive side. We recommend internalizing the relevant diagram from BSI Standard 100-4 and adapting the content to your own institution (fig. 172):

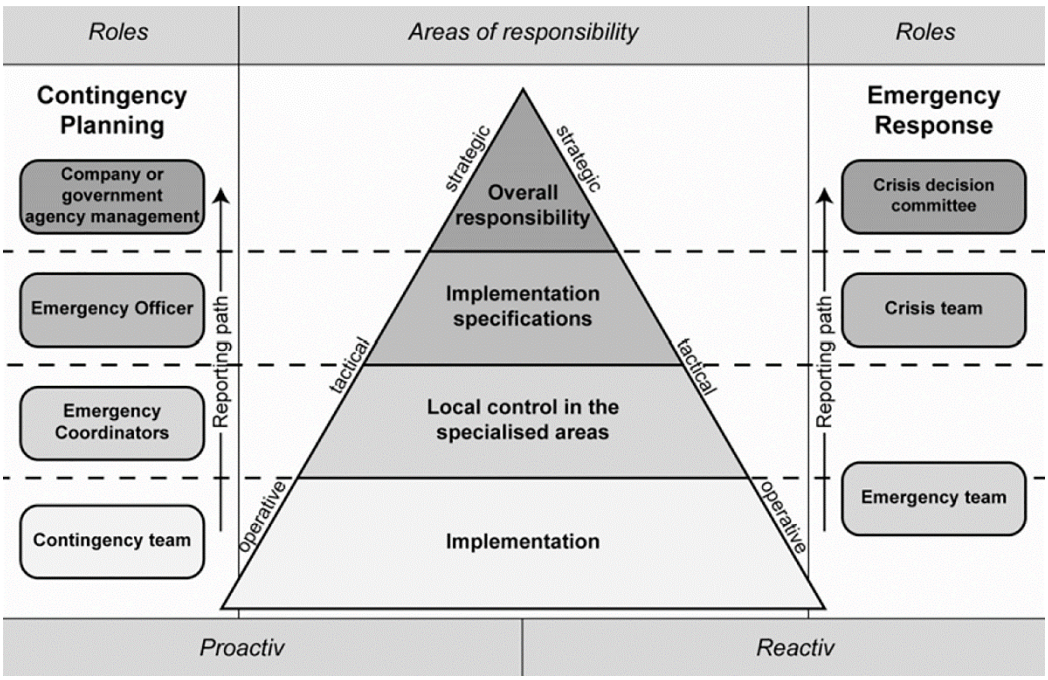


Fig. 172 Two sides of business continuity management (Proactive left, Reactive right) according to BSI Standard 100-4 (image source: BSI, [125: 23, fig. 2: Roles and areas of responsibility]).

BSI Standard 100-4 emphasizes that "not every role described […] is required in every institution" [125]. Every institution should use fig. 172 as a good starting point for adapting the roles individually—according to their size, the logical organizational structure, and the geographical distribution of the organizational units—and documenting their specific responsibilities.

The primary task of business continuity management is to maintain business operations, meaning the key business processes, which are in most cases critical. That is why the critical business processes are the focus of emergency management. “Critical”—in the context of business continuity management as defined by BSI Standard 100-4—means time-critical in the sense that “this process requires a more rapid resumption of activity, otherwise high damage to the organization can be expected.” [125]. Therefore, the business process analysis is an important entry point for both the ISMS and the BCM (see fig. 1 and table 1). It is also important to weigh up the specific impact on the organization. For this purpose, a so-called Business Impact Analysis (BIA) is generally carried out, which tries to estimate the secondary damage caused to critical business processes by an interruption in business. BSI Standard 100-4 makes it clear that there are many methods and ways to do this [125]. Starting with the master data and all the business processes, the recommendation is to select the critical processes, including the corresponding organizational units, on the basis of the following analytical steps:

- Carry out a damage analysis for the business processes.
- Define the restart parameters for the business processes.
- Take into account any interdependencies.
- Define the criticality and prioritization of business processes.
- Determine the resources for normal and emergency operation.
- Record the criticality of organizational resources and the time required to recover them.

Below is one of the key diagrams in BSI Standard 100-4 [125] (see fig. 173). It shows the time sequencing after an emergency event and identifies the essential parameters for restarting a process. These parameters are to be defined by the organization and taken into account in the emergency management and budget.

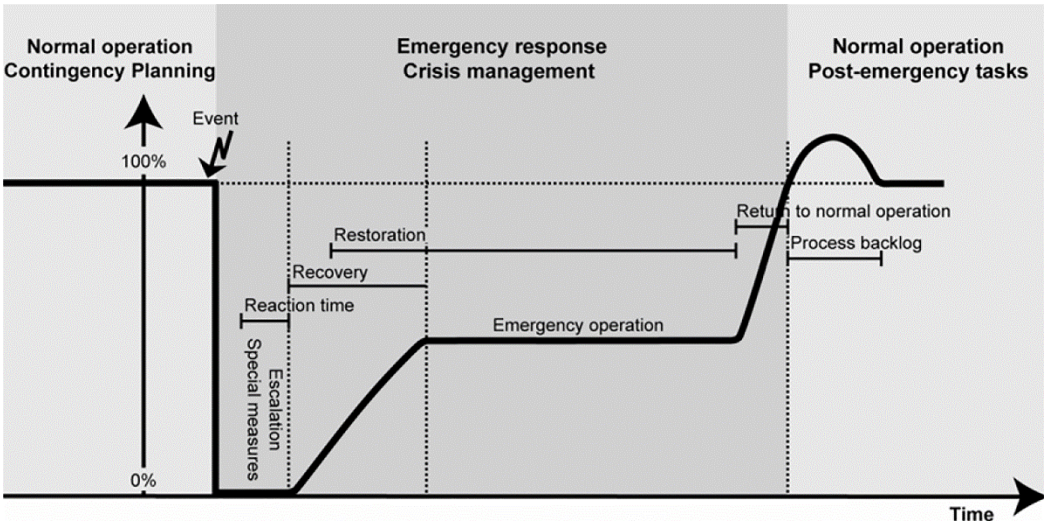


Fig. 173 Key parameters of business continuity management based on BSI Standard 100-4: these need to be defined within the organization (image source: BSI, [125: 68, fig. 9: Phases of the response to an emergency or crisis]).

Fig. 173 shows the normal operation of a business process prior to an emergency event, which causes the whole process to break down. Firstly, it is important to note when the last data backup was performed (see chapter 5.2), as this ultimately defines the maximum amount of data that can be lost. The maximum permissible data loss must therefore be defined in advance by the institution. Secondly, there is a small gap between the breakdown and reaction time, because the organization probably needs some time to register the disruption first—this must be taken into account for each critical business process in the institution. Thirdly, it is important to remember that reaction time does not equate to a restart of the business process: it indicates the time from notification of the breakdown to escalation with analysis of the actual nature of the problem and the initiation of measures to restart the process. Fourthly, the actual restart rarely occurs immediately during normal operation. It is more likely that emergency operation will kick in. The organization should thus determine in advance the maximum tolerable period of disruption (MTPD) or the recovery time objective (RTO) for each critical business process. Such definitions rely on tests and exercises if they are to be realistic. Fifthly, emergency operation will continue for a period until the actual return to normal operation can take place. This transition is what defines the maximum tolerable downtime (MTD). Sixthly, it should be noted that the recovery time can also be longer than the MTD, since it takes a certain amount of time before normal operation can be achieved again. This can take that much longer, if the incident and emergency operation have caused problems that pose an existential threat to the company. Seventhly, once normal operation is achieved, it is important to note that the work is still not finished. Rather, extra work may be necessary until the level of normal operation has been stabilized (fig. 173, right). BSI Standard 100-4 [125] recommends that the resulting extra work time should be taken into account when determining the MTPD. “If an emergency operation that lasts too long causes the extra work to become so extensive that it can no longer be carried out in a reasonable time, this can lead to further difficulties” [125].

The BSI is currently revising its Standard 100-4 and would like to introduce a step model in future called BSI Standard 200-4 [126]. Similar to the modernized basic protection, this tiered model is intended to give institutions an easier way into business continuity and emergency management. It has the following goals [126]:

- simplified entry level to lower entry barriers for institutions, facilitating the “rudimentary management” of emergencies and crises
- practical instructions for establishing a BCMS that is as comprehensive as possible, examines all business processes, and is also compatible with the international standard ISO 22301
- definition of one or more intermediate levels that facilitate the transition from entry level to an established BCMS.

In the implementation framework [127] drawn up by HiSolutions AG and the BSI, these goals are explained in detail and documented extensively.

Implementation and training exercises for awareness-raising

According to fig. 1 and table 1, the analysis of business processes is of key importance for both the ISM and the BCM. The business continuity management focuses on the critical business processes. With this in mind, exercises in business process modeling and in carrying out a BIA in connection with further training in emergency management are extremely useful. In practice, however, it should already be clear that business processes are the starting point for security considerations. These will usually not have been modeled by ISOs or BCOs but by employees from the organizational, human resources, or technical departments, which is why an exchange of ideas is recommended between the actors involved. We will not go into this further at this point. The relevant web course offered by the BSI [128] and the *DER: Detection and response* [129] module—and, more specifically, the *DER.4 Emergency Management* [130] component—in the IT-Grundschutz Compendium are suitable for trainings on BCM and emergency management.

Here, we will present two awareness-raising exercises: the first focuses on clarifying and differentiating terms, while the second deals with security incidents. For the latter, the module *DER.2.1 Handling of security incidents* [131] can be used.

Fig. 174 *"Black Out" learning scenario to raise awareness of the terms "normal operation," "disruption," "emergency," "crisis," and "catastrophe" based on BSI Standard 100-4. The board game was developed by Stefanie Gube in the elective course "Awareness of Information Security in Companies" in the summer semester 2018 at TH Wildau [132].*

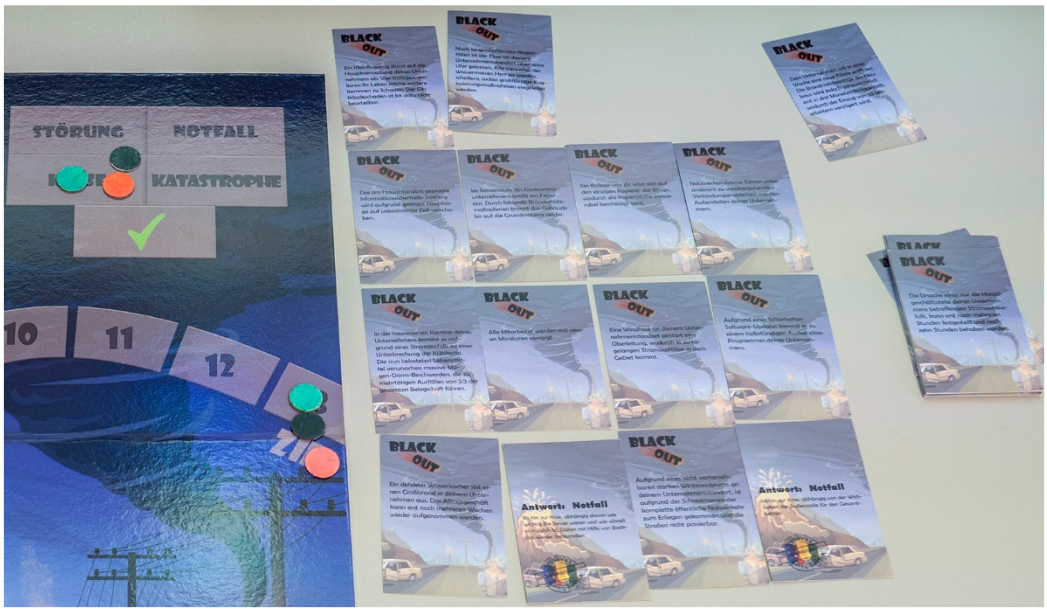


Fig. 175 *Game action in the "Black Out" learning scenario. The board and question cards were developed by Stefanie Gube in the elective course "Awareness of Information Security in Companies" in the summer semester 2018 at TH Wildau [132].*

The first learning scenario is called "Black Out" (see figs. 174 and 175). The original idea emerged from a course in the Administration and Law (VR) degree program and was developed as a pilot game by a student project team. Subsequent testing showed that the game still needs to be revised. The professionalization of the game was carried out in the following semester by Ms. Gube from the part-time Business Administration [132] program. In general, this board game is about testing the extent to which players can differentiate, on the basis of situation descriptions, between the terms "disruption," "emergency," "crisis," and "catastrophe" as defined by BSI Standard 100-4, and have an understanding of what is meant by "normal operation." A moderator holds all the question cards and reads the situation aloud. The game teams of two to three people give brief advice and place their colored chip on the term that they think is appropriate (fig. 175, top left). The moderator explains whether the answer is correct or not and places the question card on the table (fig. 175, right). The team that has bet on the correct term is allowed to move its second colored chip forward one square on the path from start to finish. The procedure is repeated with the next question card. The team that reaches the finish line first wins.

The second scenario for raising awareness on the topics presented in this chapter is called *Incident Management*: this is part of the Security Arena licensed by the company known_sense [39] and also appears in English. In our *IT-Sicherheit@KMU* project, it was adapted for German users, and in the *SecAware4job* [43] project, for English speakers based on TH Wildau's specifications (fig. 176). The analog learning scenario is divided into two phases: first, a total of twelve situation stories are read out loud and need to be correctly categorized; after that, a colored chip is assigned to the registration office that needs to be informed of the situation.

It is particularly important for players to exchange information about the extent to which they are familiar with all the reporting offices in the institution.

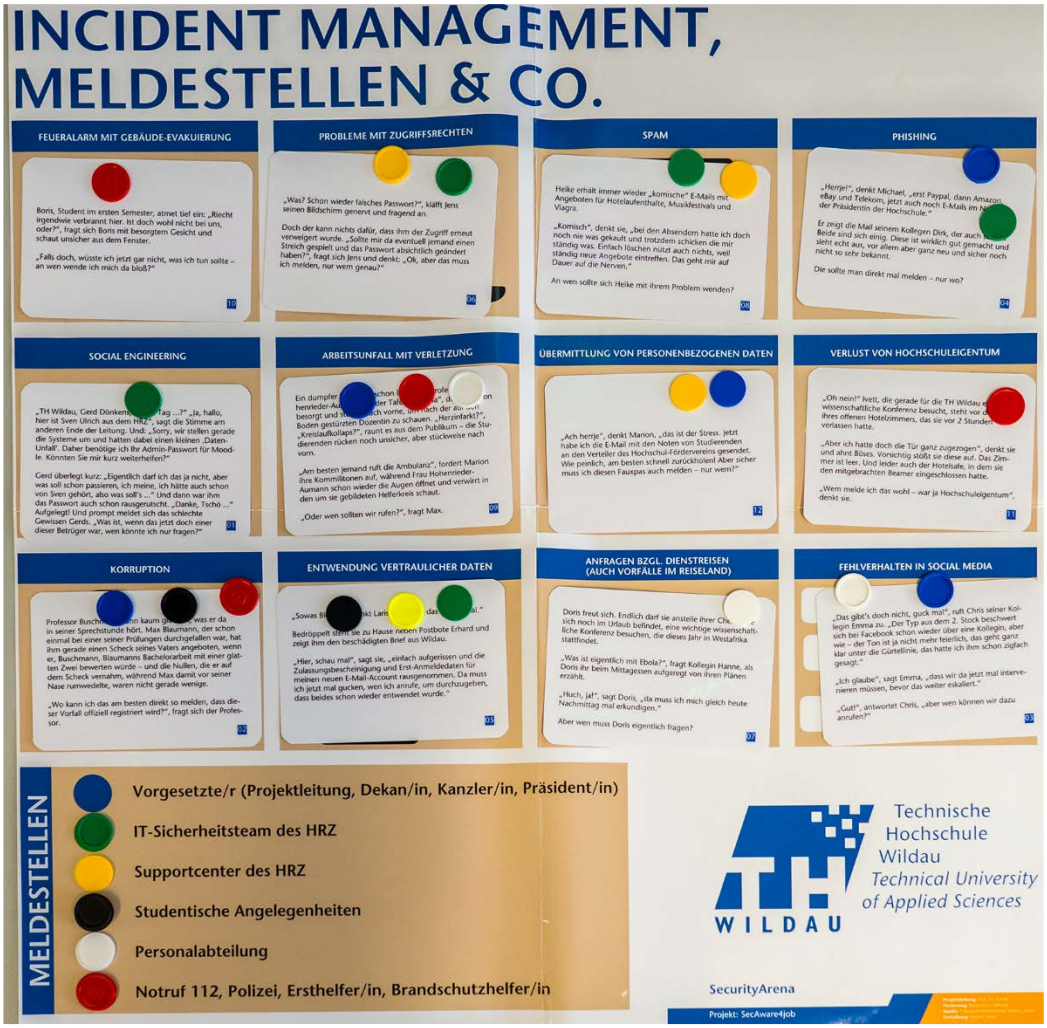


Fig. 176 Analog learning scenario "Incident Management (Reporting)" in the TH Wildau version for students. The idea comes from the Security Arena and is licensed by known_sense [39]. The game exists in different language versions.

Please test yourself using the following questions and comments for chapter 6:

- Explain the roles and responsibilities of contingency planning and emergency management.
- Explain the recovery time objective (RTO) as defined by BSI Standard 100-4.
- Explain the maximum tolerable downtime (MTD) as defined by BSI Standard 100-4.

Space for your personal comments

Personal checklist:

Personal ideas:

Personal summary:

Advantages and disadvantages:

7 References

[1] BAköV (Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern, für Bau und Heimat), **Handbuch IT-Sicherheitsbeauftragte in der öffentlichen Verwaltung**/Federal Academy of Public Administration in the Federal Ministry of the Interior, Manual IT Security Officer in Public Administration (in German), Version 6.2, 2019, Brühl.

[2] Helisch, M., and Pokoyski, D. (eds.), **Security Awareness. Neue Wege zur erfolgreichen Mitarbeiter-Sensibilisierung.** Wiesbaden: Vieweg+Teubner, 2009.

[3] Angermeier, G., **PDCA-Zyklus**, 2016. Retrieved from: https://www.projektmagazin.de/glossarterm/pdca-zyklus. Accessed: March 16, 2020.

[4] Arveson, P., **The Deming Cycle**, 1998. Retrieved from: https://balancedscorecard.org/bsc-basics/articles-videos/the-deming-cycle/. Accessed: March 16, 2020.

[5] BSI (Bundesamt für Sicherheit in der Informationstechnik), **Die Modernisierung des IT-Grundschutzes Informationssicherheit im Cyber-Raum – aktuell, flexibel, praxisnah**. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-Grundschutz-Modernisierung/Flyer_Modernisierung_des_IT-Grundschutzes.pdf?__blob=publicationFile&v=3. Accessed: March 16, 2020.

[6] IsecT Ltd. (ed.), **ISO/IEC 27000:2018 — Information technology — Security techniques — Information security management systems — Overview and vocabulary** (fifth edition). Retrieved from: https://www.iso27001security.com/html/27000.html. Accessed: March 19, 2020.

[7] **ISO/IEC 27000:2018(E)**, Information technology — Security techniques — Information security management systems — Overview and vocabulary. INTERNATIONAL STANDARD ISO/IEC 27000, fifth edition 2018-02. See: https://www.iso.org/standard/73906.html. Accessed: May 14, 2020.

[8] BSI (ed.), **IT-Grundschutz Arbeitshandbuch: DIN ISO/IEC 27001 und DIN ISO/IEC 27002, BSI-Standards 200-1/2/3**, 2nd revised edition, 459 pages. Cologne: Bundesanzeiger Verlag, October 2017.

[9] Scholl, M., Leiner, K., and Fuhrmann, F., **Blind Spot: Do You Know the Effectiveness of Your Information Security Awareness-Raising Program?** *Journal of Systemics, Informatics and Cybernetics*. Vol. 15, No. 4, pp. 58–62, 2017. Retrievable from: http://www.iiisci.org/Journal/CV$/sci/pdfs/SA199CD17.pdf. Accessed: May 14, 2020.

[10] Naumann, J., **Die ganze Härte der ISO 27001–Ihre Berufung zum Informationssicherheitsbeauftragten (ISB)**, Norderstedt: BoD, 2017.

[11] Kersten, H., Klett, G., Reuter, J., and Schröder, K. W., **IT-Sicherheitsmanagement nach der neuen ISO 27001: ISMS, Risiken, Kennziffern, Controls**. Wiesbaden: Springer Vieweg, 2nd revised edition, 2019.

[12] BSI (ed.), **IT-Grundschutz: BSI Standards**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html. Accessed: March 23, 2020.

[13] **BSI Standard 200-1 Information Security Management Systems (ISMS)**, October 2017 (in English). Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2001_en_pdf.html. Accessed: June 20, 2020.

[14] Dark, M.J., **Security Education, Training and Awareness from a Human Performance Technology Point of View**, in M.E. Whitman, and H.J. Mattord (eds.), *Readings and Cases in Management of Information Security,* Course Technology, Mason, pp. 86–104, 2006.

[15] Singh, A.N., Picot, A., Kranz, J., Cupta, M.P., and Ojha, A., **Information Security Management (ISM) Practices: Lessons from select Cases from India and Germany**, *Global Journal of Flexible Systems Management*, Vol. 14, No. 4, pp. 225–239, 2013.

[16] BSI, IT-Grundschutz-Kompendium, **Migrationsleitfaden**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/Migrationsleitfaden/Anleitung_zur_Migration_node.html. Accessed: April 20, 2020.

[17] **BSI Standard 200-2 IT-Grundschutz Methodology**, October 2017 (in English). Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2002_en_pdf.html. Accessed: June 29, 2020.

[18] **BSI Standard 200-3 Risk Analysis Based on IT-Grundschutz**, October 2017 (in English). Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/International/bsi-standard-2003_en_pdf.pdf?__blob=publicationFile&v=2. Accessed: July 2, 2020.

[19] BSI, **IT-Grundschutz-Schulungen, Online-Kurs: Informationssicherheit mit IT-Grundschutz**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Schulung/itgrundschutzschulung_node.html. Accessed: March 23, 2020.
Lerneinheit 7.7: Risiken bewerten. Retrieved from: https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/ITGrundschutzSchulung/OnlinekursITGrundschutz2018/Lektion_7_Risikoanalyse/Lektion_7_07/Lektion_7_07_node.html. Accessed: March 23, 2020.

[20] BSI, **IT-Grundschutz-Kompendium**. Retrieved from: https://www.bsi.bund.de/DE/Themen/IT-Grundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html. Accessed: March 26, 2020.

[21] BSI, IT-Grundschutz-Kompendium, **Baustein ISMS.1 Sicherheitsmanagement**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ISMS/ISMS_1_Sicherheitsmanagement.html. Accessed: March 25, 2020.

[22] BSI, **Umsetzungshinweise zum IT-Grundschutz-Kompendium 2019**, Community Drafts, February 4, 2019. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.html. Accessed: March 25, 2020.

[23] BSI, **IT-Grundschutz-Kompendium, Zweite Edition Februar 2019 als PDF**. Köln: Bundesanzeiger Verlag, Reguvis. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2019.pdf?__blob=publicationFile&v=5. Accessed: April 3, 2020.

[24] BSI, **Checklisten Handbuch IT-Grundschutz**, Prüfaspekte des IT-Grundschutz-Kompendiums, 2nd edition, 4th revised version. Cologne: Bundesanzeiger Verlag, 2019.

[25] BSI, **Checklisten zum IT-Grundschutz-Kompendium der Edition 2019**, 04.02.2019. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/checklisten_2019.html. Edition 2019. Accessed: March 26, 2020.

[26] https://verinice.com/. Accessed: March 27, 2020.

[27] BSI, IT-Grundschutz-Kompendium, **Baustein ORP.3 Sensibilisierung und Schulung**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_3_Sensibilisierung_und_Schulung.html. Accessed: April 3, 2020.

[28] Scholl, M. C., Fuhrmann, F., and Scholl, L. R., **Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices**, Proceedings of *The 52th Hawaii International Conference on System Sciences (HICSS)*, 2018. Retrievable from: https://scholarspace.manoa.hawaii.edu/handle/10125/50168. Accessed: April 3, 2020.

[29] Kruger H., Drevin, L., and Steyn, T., **Email Security Awareness: A Practical Assessment of Employee Behaviour**, in L. Futcher, and R. Dodge (eds.), *Fifth World Conference on Information Security Education. IFIP – International Federation for Information Processing*, Vol. 237, Springer, Boston, MA, pp. 33–40, 2007.

[30] Aytes, K., and Terry, C., **Computer Security and Risky Computing Practices: A Rational Choice Perspective**, *Journal of Organizational and End User Computing*, Vol. 16, No. 3, pp. 22–40, 2004.

[31] Kim, E.B., **Recommendations for Information Security Awareness Training for College Students**, *Information Management & Computer Security*, Vol. 22, No. 1, pp. 115–126, 2014.

[32] Styles, M., **Constructing Positive Influences for User Security Decisions to Counter Corporate or State Sponsored Computer Espionage Threats**, in L. Marinos and I. Askoxylakis (eds.), *Human Aspects of Information Security, Privacy, and Trust*, HAS 2013, Lecture Notes in Computer Science, Vol. 8030, Berlin, Heidelberg: Springer, pp. 197–206, 2013.

[33] Warkentin, M., Johnston, A.C., and Shropshire, J., **The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention**, *European Journal of Information Systems,* Vol. 20, No. 3, pp. 267–284, 2011.

[34] Beyer, M., Ahmed, S., Doerlemann, K., Arnell, S., Parkin, S., Sasse, A., and Passingham, N., **Awareness Is Only the First Step: A Framework for Progressive Engagement of Staff in Cyber Security**, Hewlett Packard, *Business white paper*, 2016.

[35] Karjalainen, M., Siponen, M., and Sarker, S., **Towards a Stage Theory of the Development of Employees' Information Security Behavior**, *Computers & Security*, 93, 101782. DOI: 10.1016/j.cose.2020.101782, 2020.

[36] Khan, B., Alghathbar, K.S., Nabi, S.I., and Khan, M.K., **Effectiveness of Information Security Awareness Methods Based on Psychological Theories**, *African Journal of Business Management*, Vol. 5, No. 26, pp. 10862–10868, 2011.

[37] Scholl, M., Fuhrmann, F., and Pokoyski, D., **Information Security Awareness 3.0 for Job Beginners**, in J. E. Varajão, M.M. Cruz-Cunha, R. Martinho, R. Rijo, N. Bjørn-Andersen, R. Turner, and D. Alves (eds.), *Conference on ENTERprise Information Systems (CENTERIS)*, pp. 433–436, 2016

[38] BAköV (ed.), **"Sicher gewinnt"–auch in Zukunft: Sensibilisierungsinitiative für Informationssicherheit in der Bundesverwaltung**. Retrieved from: https://www.bakoev.bund.de/DE/02_Themen/Informationstechnik/sicher_gewinnt/sicher_gewinnt.html. Accessed: April 5, 2020.

[39] http://www.known-sense.de. Accessed: April 5, 2020.

[40] https://www.lernplattform-bakoev.bund.de/index.php?client_id=BAKOEV. (Currently not accessible)

[41] BSI (ed.), **Umsetzungshinweise zum Baustein ORP.3 Sensibilisierung und Schulung**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/ORP/Umsetzungshinweise_zum_Baustein_ORP_3_Sensibilisierung_und_Schulung.html. Accessed: April 5, 2020.

[42] BSI, **Umsetzungshinweise_Kompendium_CD_2019**. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Umsetzungshinweise_Kompendium_CD_2019.pdf?__blob=publicationFile&v=10. Accessed: April 13, 2020.

[43] https://secaware4job.wildau.biz. Accessed: April 6, 2020.

[44] https://szenarien.wildau.biz. Accessed: April 6, 2020.

[45] Fuhrmann, F., Scholl, M., Edich, D., Koppatz, P., Scholl, L.R., Leiner, K.B., and Ehrlich, E.P., **Abschlussbericht Informationssicherheit für den Berufseinstieg (SecAware4job)**, edited by M. Scholl. Düren: Shaker Verlag, 2017. Retrievable from: http://www.shaker.de/de/content/catalogue/index.asp?lang=&ID=8&ISBN=978-3-8440-5466-8. Accessed: April 6, 2020.

[46] https://security.wildau.biz. Accessed: April 6, 2020.

[47] Prott, F., Edich, D., and Gerlach, J., **Informationssicherheit: Ein Berufsfeld mit Zukunft**. The brochure (in German) can be downloaded from the project website [46]. Accessed: April 3, 2020.

[48] Scholl, M., and Prott, F. (eds.), **Jeder Tag sieht anders aus: Aus dem Leben von Informationssicherheits-Spezialistinnen**. Düren: Shaker Verlag, 2020. Retrievable from: https://www.shaker.de/de/content/catalogue/index.asp?lang=de&ID=8&ISBN=978-3-8440-6712-5&search=yes. Accessed: July 25, 2020.

[49] https://szenarien.wildau.biz/security_sketch_passwords/story_html5.html. In German. Accessed: April 6, 2020.

[50] Prott, F., Scholl, M., Edich, D., and Gerlach, J., **Projektdokumentation Gendersensible Studien- und Berufsorientierung für den Beruf Security Spezialistin (Security)**, edited by M. Scholl. Düren: Shaker Verlag, 2020. Retrievable from: https://www.shaker.de/de/content/catalogue/index.asp?lang=de&ID=8&ISBN=978-3-8440-7133-7&search=yes. Accessed: July 25, 2020.

[51] https://secaware4school.wildau.biz. Accessed: April 6, 2020.

[52] Schuktomow, R., Scholl, M., Gube, S., Koppatz, P., Edich, D., and Gerlach, J., **Informationssicherheitsbewusstsein für den Schulalltag (SecAware4school)**, edited by M. Scholl. Frankfurt am Main: Buchwelten-Verlag, 2020. Retrievable from: https://buchwelten-verlag.de/books.php, in print, October 2020.

[53] https://szenarien.wildau.biz/security_sketch_passwords_eng/story_html5.html. In English. Accessed: April 7, 2020.

[54] https://diz.wildau.biz. Accessed: April 6, 2020.

[55] BSI, IT-Grundschutz-Kompendium, **Baustein INF: Infrastruktur**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_Uebersicht_node.html. Accessed: April 11, 2020.

[56] BSI, IT-Grundschutz-Kompendium, **Baustein ORP.4 Identitäts- und Berechtigungsmanagement**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/ORP/ORP_4_Identitäts-_und_Berechtigungsmanagement.html. Accessed: April 11, 2020.

[57] BSI (ed.), **Radio Frequency Identification (RFID)**. Retrieved from: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/RadioFrequencyIdentification/radiofrequencyidentification_node.html. Accessed: May 20, 2020.

[58] Ratter, D., Zeskowski, P., Schröder, A., Walter, T., Thiel, B., and Walter, J., **Smart Home sicher nutzen**, assignment paper in the course *Information security and awareness* (in German), TH Wildau, WS 2018/2019, 22.01.2019.

[59] BSI, IT- Grundschutz-Kompendium, **Baustein CON.7 Informationssicherheit auf Auslandsreisen**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/CON/CON_7_Informationssicherheit_auf_Auslandsreisen.html. Accessed: April 13, 2020.

[60] The Wirtschaftsschutz Initiative provides further information on its website, https://www.wirtschaftsschutz.info, including on security on business trips. Accessed: May 20, 2020.

[61] Bartels, J., Kubitz, S., Lange, L., and Weltjen, S., **Konzept zur Sensibilisierung – Arbeiten in öffentlichen Umgebungen**, assignment paper in the course *Information security and awareness* (in German), TH Wildau, WS 2019/2020, 19.01.2020

[62] BSI, IT-Grundschutz-Kompendium, **Elementare Gefährdungen, G 0.42 Social Engineering**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/elementare_gefaehrdungen/G_0_42_Social_Engineering.html. Accessed: April 14, 2020.

[63] known_sense, LanXess, TH Wildau, and <kes>, **Bluff me if U can–Gefährliche Freundschaften am Arbeitsplatz: Tiefenpsychologische Wirkungsanalyse Social Engineering und seine Abwehr**, study, 2015. A part of the study is retrievable from: http://www.known-sense.de/Bluff-MeIfUCanAuszug.pdf. Accessed: April 15, 2020.

[64] https://secaware4job.wildau.biz/ds/se/story_html5.html. Accessed: April 15, 2020.

[65] Gießmannn N., Gerlich, L., Müller, K., Lorenz, L.E., and Röhm, J., **Social Engineering Awareness –Jeder kann gehackt werden**, assignment paper in the course *Information security and awareness* (in German), TH Wildau, WS 2018/2019, 23.01.2019.

[66] Darkow, M., Krüger, R., Wernitz, R., and Zimmermann, C., **Konzept Sensibilisierung für Informationssicherheit: Vorbeugen gegen Social Engineering**, assignment paper in the course *Information security and awareness* (in German), TH Wildau, WS 2019/2020, 24.01.2020.

[67] BSI (ed.), **Passwortdiebstahl durch Phishing**. Retrieved from: https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/SpamPhishingCo/Phishing/phishing_node.html. Accessed: April 15, 2020.

[68] BSI für Bürger (BSI for citizens), **Vorsicht Phishing: Die Corona-Krise als Köder**. Retrieved from: https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/phishing-corona.html. Accessed: April 15, 2020.

[69] https://secaware4job.wildau.biz/ds/ph4/story_html5.html. Accessed: April 15, 2020.

[70] https://szenarien.wildau.biz/terminal-hacker/. Accessed: April 12, 2020.

[71] https://szenarien.wildau.biz/security_sketch_passwords_eng/story_html5.html. Accessed: July 12, 2020.

[72] https://www.gesetze-im-internet.de/stgb/index.html. Accessed: April 15, 2020.
https://secaware4job.wildau.biz/ds/hangman/. Accessed: April 15, 2020.

[73] BSI, IT-Grundschutz-Kompendium, **Baustein CON.3 Datensicherungskonzept**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_3_Datensicherungskonzept.html. Accessed: April 17, 2020.

[74] BSI, IT-Grundschutz-Kompendium, **Baustein OPS.1.2.2 Archivierung**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_2_2_Archivierung.html. Accessed: April 17, 2020.

[75] BSI, **Technische Richtlinien**. Retrieved from: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/technischerichtlinien_node.html. Accessed: April 17, 2020.

[76] BSI, **Technische Richtlinie TL03420: Leitlinie für das Löschen und Vernichten von Verschlusssachen auf Datenträgern**, 2014, Module *CON.6 Löschen und Vernichten*.
Technical guideline TL03420: Guideline for the Deletion and Destruction of Encrypted Information on Data Media, in German, 2014. The BSI has now developed the *CON.6 deletion and destruction module.* Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_6_L%C3%B6schen_und_Vernichten.html. Accessed: June 12, 2020.

[77] Hansen, H.R., and Neumann, G., **Wirtschaftsinformatik 1**, 10., fully r evised, UTB, Stuttgart. Based on fig. 8.1/1: Merkmale von Datenträgern, p. 702, 2009.

[78] Balzert, H., **Lehrbuch der Softwaretechnik: Softwaremanagement**, Spektrum Akademischer Verlag, 2008.

[79] BSI, *IT-Grundschutz Compendium* (in German), **Baustein CON.4 Auswahl und Einsatz von Standardsoftware**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_4_Auswahl_und_Einsatz_von_Standardsoftware.html.
Accessed: May 16, 2020.

[80] BSI, *IT-Grundschutz Compendium* (in German), **Baustein CON.5 Entwicklung und Einsatz von Individualsoftware**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_5_Entwicklung_und_Einsatz_von_Individualsoftware.html. Accessed: May 16, 2020.

[81] BSI, *IT-Grundschutz Compendium* (in German), **Baustein CON.8 Software-Entwicklung**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_8_Software-Entwicklung.html. Accessed: May 16, 2020.

[82] BSI, *IT-Grundschutz Compendium* (in German), **Baustein OPS.1.1.3 Patch- und Änderungsmanagement**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/OPS/OPS_1_1_3_Patch-_und_Änderungsmanagement.html. Accessed: May 16, 2020.

[83] BSI, *IT-Grundschutz Compendium* (in German), **Baustein OPS.1.1.4 Schutz vor Schadprogrammen**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/OPS/OPS_1_1_4_Schutz_vor_Schadprogrammen.html. Accessed: May 16, 2020.

[84] BSI, *IT-Grundschutz Compendium* (in German), **Baustein OPS.1.1.6 Software-Tests und -Freigaben**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutz-Kompendium/bausteine/OPS/OPS_1_1_6_Software-Tests_und_-Freigaben.html. Accessed: May 16, 2020.

[85] BSI, *IT-Grundschutz Compendium* (in German), **Baustein APP: Anwendungen**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_Uebersicht_node.html. Accessed: May 16, 2020.

[86] BSI, *IT-Grundschutz Compendium* (in German), **Baustein APP.1.1 Office-Produkte**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/APP/APP_1_1_Office-Produkte.html. Accessed: May 16, 2020.

[87] Dorn, L., Koschel, H., Lang, J., Müller, S., Thiem, J., and Westphal, V., **Schadsoftware**, assignment paper in the course *Information security and awareness* (in German), degree program Administration Informatics (VIBB-18), TH Wildau, WS 2018/2019, January 22, 2019.

[88] Szukala, P., Lohse D., and Markus, F., **Videospiele sicher nutzen**, assignment paper in the course *Information security and awareness* (in German), degree program Administration Informatics (VIBB-18), TH Wildau, WS 2018/2019, January 22, 2019.

[89] Bundesverfassungsgericht (ed.), **Verfassungsbeschwerden gegen § 202c Abs. 1 Nr. 2 StGB unzulässig**. Retrieved from: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2009/bvg09-067.html. Accessed: May 16, 2020.

[90] https://gist.github.com/worawit/77a839e3e5ca50916903. Accessed: May 16, 2020.

[91] BAköV, **Handbuch Behördliche Datenschutzbeauftragte in der Bundesverwaltung**, Version 2.0, Brühl, 2018. See also https://gdpr-info.eu/art-6-gdpr/

[92] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016. For example: **Article 6 Lawfulness of processing**. Retrieved from: https://eur-lex.europa.eu/legal-content/en/TXT/HTML/?uri=CELEX:32016R0679/. Accessed: September 1, 2020.

[93] BSI, *IT-Grundschutz Compendium* (in German), **Baustein CON.2 Datenschutz**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/CON/CON_2_Datenschutz.html. Accessed: May 9, 2020.

[94] Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), **Standard-Datenschutzmodell (SDM)**, Version 2b. Retrieved from: https://www.datenschutzzentrum.de/sdm/. Accessed: May 9, 2020.

[95] Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, **Bausteine der SDM-Version 1.0**. Retrieved from: https://www.datenschutz-mv.de/datenschutz/datenschutzmodell/. Accessed: May 9, 2020.

[96] Der Landesbeauftragte für Datenschutz und Informationsfreiheit Mecklenburg-Vorpommern, **Baustein 43 "Protokollierung."** Retrieved from: https://www.datenschutz-mv.de/static/DS/Dateien/Datenschutzmodell/Bausteine/SDM-V1.1_43_Protokollierung_V1.0_uagsdmbs_final.pdf. Accessed: May 9, 2020.

[97] **Anleitung zum deutschsprachigen Serious Game: Brettspiel "Keep your data private. Everyday."** Instructions for the German Serious Board Game "Keep your data private. Everyday." Developed as a part of the project *SecAware4job* [43], 2018.

[98] https://creativecommons.org/licenses/by-nc-sa/2.0/de/. Accessed: May 9, 2020.

[99] https://szenarien.wildau.biz/bildrechte/#/. Accessed: May 9, 2020.

[100] Bielig, A., Hesse, A., **Sensibilisierungsmaßnahme zum Thema "Videoüberwachung,"** assignment paper in the course *IT security and data protection law* (in German), degree program Public Administration Brandenburg (ÖVBB-16/2), TH Wildau, SS 2019, 11.05.2019.

[101] Frank, F., Selle, A., **Moderationsleitfaden zum Thema "Videoüberwachung,"** assignment paper in the course *IT security and data protection law* (in German), degree program Public Administration Brandenburg (ÖVBB-16/1), TH Wildau, SS 2019.

[102] Cabañas, I., Calderon, V., Eppers, S., Funk, S., Raic, A., Kumi-Dumor, E., and Urazbakhtina A., **N°83 NOT JUST A GAME–IT´S THE LAW**, assignment paper in the course *Project Management* (in English), degree program European Management Master (EMM-17), TH Wildau, WS 2017/18.

[103] Künkel, J., Büge, I., Udhardt, S., Brama, M., Hüsing, E., and Lopez, G.M., **Concept of the game based learning scenario**, assignment paper in the course *Project Management* (in English), degree program European Management Master (EMM-17), TH Wildau, WS 2017/18.

[104] Özoktaş, E., Halle, E., Carrasco, F., Aigner, H., Chomicka, K., Zunk, L., and Kurt, O., **Interactive teaching methods: Data protection**, assignment paper in the course *Project Management* (in English), degree program European Management Master (EMM-17), TH Wildau, WS 2017/18.

[105] Beran, T., Vanegas, L.P., Scheel, N.C., Schulz, C., Henning, K., and Mandra, S., **Game Based Learning Scenario**, assignment paper in the course *Project Management* (in English), degree program European Management Master (EMM-17), TH Wildau, WS 2017/18.

[106] Baatz, S., Rosinsky, R., Freund, S., Worm, C., Hinterschuster, J., Lehmann, K., and König, D., **Spielanleitung EU-DSGVO-Memo**, assignment paper in the course *E-Government Project Work* (in German), degree program Administration and Law (VR-15), TH Wildau, WS 2017/18.

[107] BSI & BBK (eds.), **Kritische Infrastrukturen–Definition und Übersicht**. Retrieved from: https://www.kritis.bund.de/SubSites/Kritis/DE/Einfuehrung/einfuehrung_node.html. Main page: https://www.kritis.bund.de/SubSites/Kritis/DE/Home/home_node.html. Accessed: May 16, 2020.

[108] Güttich, G., and Schmitz, P., **IT-Sicherheit in Staat und Verwaltung–Netzwerksicherheit beim Landkreistag**, *Security Insider*, 15.05.2020. Retrieved from: https://www.security-insider.de/netzwerksicherheit-beim-landkreistag-a-930844/?cmp=nl-36&uuid=3B10C402-D57C-4A08-8E093243626CC222. Accessed: May 18, 2020.

[109] Güttich, G., and Schmitz, P., **Anforderungen der IT-Sicherheit–Grundlagen der Netzwerksicherheit**, *Security Insider*, 12.04.2019. Retrieved from: https://www.security-insider.de/grundlagen-der-netzwerksicherheit-a-818810/. Accessed: May 18, 2020.

[110] https://www.netzwerke.com/OSI-Schichten-Modell.htm. Accessed: May 18, 2020.

[111] BSI, *IT-Grundschutz Compendium* (in German), **Baustein NET.3.1 Router und Switches**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_1_Router_und_Switches.html. Accessed: May 18, 2020.

[112] BSI, *IT-Grundschutz Compendium* (in German), **Baustein NET.3.2 Firewall**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_2_Firewall.html. Accessed: May 18, 2020.

[113] BSI, *IT-Grundschutz Compendium* (in German), **Baustein NET.1.1 Netzwerkarchitektur und -design**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_1_1_Netzarchitektur_und_-design.html. Accessed: May 18, 2020.

[114] BSI, *IT-Grundschutz Compendium* (in German), **Baustein NET.3.3 VPN**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_3_3_VPN.html. Accessed: May 18, 2020.

[115] BSI, *IT-Grundschutz Compendium* (in German), **Baustein INF.9 Mobiler Arbeitsplatz**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/INF/INF_9_Mobiler_Arbeitsplatz.html. Accessed: May 18, 2020.

[116] BSI, *IT-Grundschutz Compendium* (in German), **Baustein NET.2.1 WLAN-Betrieb**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_2_1_WLAN-Betrieb.html. Accessed: May 18, 2020.

[117] Gebur, S., **Entwicklung eines "Game-Based" Lernszenarios zum Thema DDoS-Angriff**. Bachelor Thesis (in German), TH Wildau, 15.08.2019.

[118] BSI, **Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 1**, Version: 2020-01. Retrieved from: https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html. Accessed: May 13, 2020.

[119] BSI, **Technical Guideline TR-02102-4, Cryptographic Mechanisms: Part 1–Recommendations and Key Lengths,**
Part 2–Use of Transport Layer Security (TLS)
Part 3–Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)
Part 4–Use of Secure Shell (SSH), 2020.
Retrieved from:
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html.
Accessed: May 13, 2020.

[120] Singh, S., **Geheime Botschaften**, dtv, 10th edition, 2011.

[121] https://www.gpg4win.de/download-de.html. Accessed: May 25, 2020.

[122] https://www.chip.de/downloads/PGP-Desktop_12994029.html. Accessed: May 25, 2020.

[123] BSI, **Erstellung von Kryptokonzepten**, Version 1.0, 2008. Retrieved from: https://www.bsi.bund.de/DE/Themen/Sicherheitsberatung/Arbeitshilfen/Krytokonzept/Kryptokonzept_node.html. Accessed: May 13, 2020.

[125] **BSI Standard 100-4 Business Continuity Management**, 2009. Retrieved from: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutz-standards/BSI-Standard_1004.pdf?__blob=publicationFile&v=2. Accessed: May 14, 2020.

[126] BSI, **Aktueller Informationsstand zur Weiterentwicklung des BSI-Standards 200-4**, April 2019. Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BCM/BCM_20190416_Infomail.pdf?__blob=publicationFile&v=2. Accessed: May 14, 2020.

[127] BSI, **Umsetzungsrahmenwerk zum Notfallmanagement nach BSI-Standard 100-4**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Umsetzungsrahmenwerk/umra_node.html. Accessed: May 14, 2020.

[128] BSI, **Online-Fortbildung, Webkurs Notfallmanagement nach BSI-Standard 100-4**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/Webkurs1004/Webkurs1004_node.html. Accessed: May 15, 2020

[129] BSI, *IT-Grundschutz Compendium* (in German), **Baustein DER: Detektion und Reaktion**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_Uebersicht_node.html. Accessed: May 15, 2020.

[130] BSI, *IT-Grundschutz Compendium* (in German), **Baustein DER.4 Notfallmanagement**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_4_Notfallmanagement.html. Accessed: May 15, 2020.

[131] BSI, *IT-Grundschutz Compendium* (in German), **Baustein DER.2.1 Behandlung von Sicherheitsvorfällen**. Retrieved from: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/DER/DER_2_1_Behandlung_von_Sicherheitsvorfällen.html. Accessed: May 15, 2020.

[132] Gube, S., **Black Out und I•SOS: - Evaluation und Optimierung zweier spielebasierter Sensibilisierungsmaßnahmen für Informationssicherheit**, project work as part of the optional course *Awareness for Information Security in Enterprises*, in the part-time business administration course (in German: *Betriebswirtschaft)*, TH Wildau, SS 2018.

8 List of figures

9 List of tables

10 List of abbreviations

AES	Advanced Encryption Standard (symmetrisches Verschlüsselungsverfahren)
BAköV	Federal Academy for Public Administration in the Federal Ministry of the Interior [in German: Bundesakademie für öffentliche Verwaltung im Bundesministerium des Innern (BMI)]
BCM	Business Continuity Management
BCO	Business Continuity Officer (emergency officer; in German: Notfallbeauftragte/r)
BDSG	Federal Data Protection Act (Germany) [in German: Bundesdatenschutzgesetz (Deutschland)]
BfDI	Federal Commissioner for Data Protection and Freedom of Information [in German: Bundesbeauftragte für den Datenschutz und die Informationsfreiheit]
BIA	Business Impact Analysis
BMBF	Federal Ministry of Education and Research [in German: Bundesministerium für Bildung und Forschung]
Botnet	Connection of remote-controlled computers (for attacks)
BSI	Federal Office for Information Security [in German: Bundesamt für Sicherheit in der Informationstechnik]
CC	Creative Commons (license information)
DDoS	Distributed Denial of Service (attack)
DIZ	Digitization Center (for business in Stuttgart, State of Baden Württemberg, Germany) [in German: Digitalisierungszentrum (DIZ) Stuttgart]
DMZ	“Demilitarized zone” (separate area in the network architecture)
DNS	Domain Name System
DP	Data protection
DPO	Data Protection Officer
GDPR	General Data Protection Regulation (of the EU)
FS	Research Group Scholl [in German: Forschungsgruppe Scholl (FS)]
FZI	Research Center for Computer Science (in Karlsruhe, State of Baden Württemberg, Germany) [in German: Forschungszentrum Informatik]
HGS	Horst Görtz Foundation [in German: Horst Görtz Stiftung]
HRZ	University data center [in German: Hochschulrechenzentrum]
ICS	Industrial Control System
INF	(BSI *IT-Grundschutz Compendium* module) Infrastructure
IoT	Internet of Things
IP	Internet Protocol
IS	Information security
ISA	Information security awareness
ISAT	Information security awareness training
ISO	Information Security Officer
ISM	Information security management
ISMS	Information security management system
IT	Information technology
LDSG	State data protection law[s] (Germany) [in German: Landesdatenschutzgesetz[e] (Deutschland)]
OSI	Open Systems Interconnection (layer model of electronic communication)

PKI	Public Key Infrastructure
RSA	Asymmetrical encryption method of Rivest, Shamir, and Adleman
SAN	Storage area network
SE	Social engineering
SHA	Secure hash algorithm
SLA	Service level agreement
SME	Small and medium-sized enterprises
SoA	Statement of Applicability
SPAM	or JUNK (unwanted advertising email)
SSL	Secure Sockets Layer
TOM	Technical and organizational measures
TLS	Transport Layer Security
TWZ	Technology Transfer and Continuing Education Center at TH Wildau [in German: Technologietransfer- und Weiterbildungszentrum an der TH Wildau e.V.]
ULD	Independent state center for data protection Schleswig-Holstein [in German: Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein]
UP Bund	Federal administration implementation plan [in German: Umsetzungsplan (UP) Bundesverwaltung]
UPS	Uninterruptible power supply [in German: unterbrechungsfreie Stromversorgung (USV)]
URL	Uniform Resource Locator
VB	Visual Basic
VLAN	Virtual Local Area Network
VPN	Virtual private network
WILLE	Wildau Institute for Innovative Teaching, Lifelong Learning, and Evaluation [in German: Wildau Institut für innovative Lehre, lebenslanges Lernen und gestaltende Evaluation]
WLAN	Wireless Local Area Network

Short biography of the editor

Margit Christa Scholl (Prof. Dr. rer. nat.)

After studying physics and meteorology in Mainz and Berlin, Margit Scholl worked as a scientist for the German Research Foundation on a series of projects in the 1980s. She developed and processed numerical models for weather forecasting and pollutant dispersion with the help of digital satellite imagery. She did her doctorate in meteorology at the Freie Universität in Berlin. Margit Scholl has two sons.

After graduating from university, she held a number of positions, including a stint as the head of a unit in the Berlin administration. In her free time, she continued her education in business administration and computer sciences through distance learning. In 1994, she received a professorship at the Bernau University of Applied Sciences in Brandenburg and helped transfer the pilot courses for public administration to the Technical University of Applied Sciences Wildau, today's TH Wildau, in 1997. She then became the head of IT first-level support in what is now ZIT-BB and briefly supported the Federal University of Applied Sciences for Public Administration in Berlin.

In 2001, she returned to TH Wildau as a professor for business and administrative informatics in the Department of Business, Administration, and Law (FB WIR). In addition to IT and enterprise applications, project management, and e-government, her specific research focuses are information technology and digital science, infrastructures, conducive learning, individual and organizational learning, and digital media.

In 2010, she founded WILLE—the Wildau institute for innovative teaching, lifelong learning, and creative evaluation. This also gave her research group a new focus: on information security and data protection and awareness. As a highly active research professor, she received her university's research award in 2011, spent a research semester in 2013 at the iSchool of the University of Washington in Seattle, USA, and received a five-year research professorship at TH Wildau in 2014. Her goal in this new position was to develop a holistic understanding of technology. Since then, she has implemented this principle both in teaching and in other third-party funded projects.

Congratulations on your new job as an information security officer!

What does this responsibility actually entail? How will you manage not to get bogged down? How are you going to keep all the relevant issues in mind? How will you get started?

This book is intended to help you take a holistic approach to information security while retaining an overview of the topic. Its primary aim is to impart the essentials of the IT-Grundschutz approach—both as theory and practice—as per the BSI standards 200-x. This book not only serves as a practical guide to basic protection but also allows you to reproduce the procedure on your own computer as a mini scenario.

Another focus is on awareness-raising trainings for employees of your institution targeted at specific groups. These trainings will need to be individually initiated, planned, implemented, and evaluated. We deal with the relevant technical and organizational aspects and focus on a discursive learning atmosphere devoted to interpersonal exchange, experience-oriented learning scenarios, and practical demonstrations designed to achieve a sustained effect and benefit all employees.

Have fun reading and good luck with implementing the ideas!

ISBN 978-3-945740-12-5

9 783945 740125

ISBN 978-3-945740-12-5

The printing of this book was funded by the Horst Görtz Foundation (HGS) as part of the project "Information Security Awareness for Everyday School Life (SecAware4school)."

Buchwelten Verlag
FRANKFURT AM MAIN