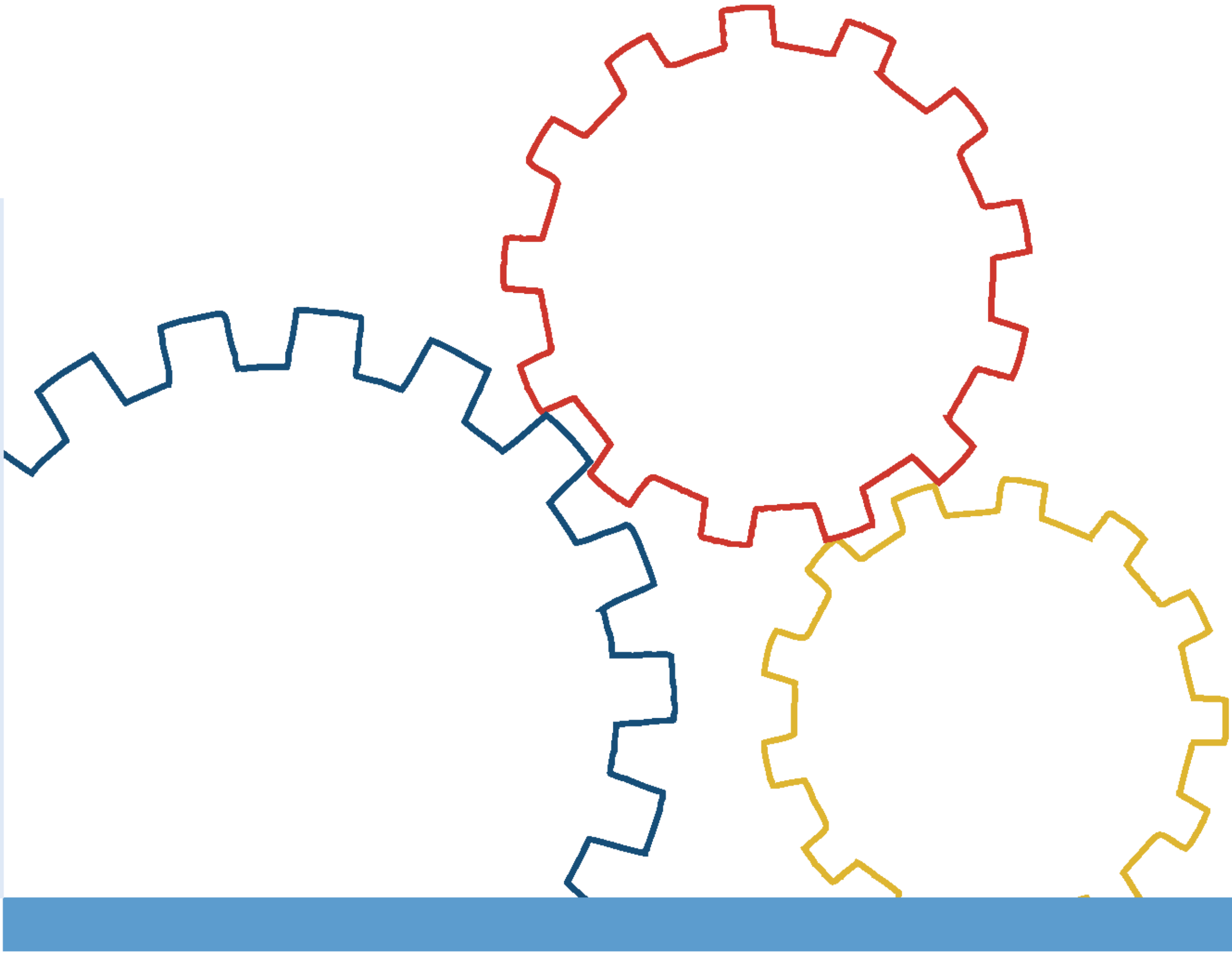
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 200-1

Information Security Management Systems (ISMS)



www.bsi.bund.de/grundschutz

Version 1.0

BSI Standard 200-1

Information Security Management Systems (ISMS)

Version 1.0, October 2017

Federal Office for Information Security (BSI)
Godesberger Allee 185-189, 53175 Bonn, Germany

Table of contents

1 Introduction

1 Introduction

1.1 Version history

BSI standard 200-1 supersedes BSI standard 100-1.

As per	Version	Changes
April 2017	CD 1.0	Updated based on BSI standard 100-1 • Adaptations to updated ISO standards • Adaptations to BSI standard 200-2 (IT-Grundschutz methodology)
October 2017	V 1.0	User comments incorporated • substantially language-related clarifications • Differentiation between the German terms Norm and Standard

1.2 Objective

Today, the increasing digitalisation and networking of the work environment presents companies and government agencies with fundamental challenges. Likewise, the basic threat situation for information security in companies and government agencies is very dynamic and diverse. In order to be able to operate business processes or specialised tasks with the help of IT, whether offline or online, in a secure manner and to thus also be competitive in the long run, organisations must increasingly address the questions in the field of information security in an improved manner. The developments in the field of information technology today are characterised by shorter and shorter innovation cycles. Likewise, the technical systems are characterised by an increased complexity. The dependency on working technology is increasing in more and more areas of public and business life. The networking and control of industrial facilities, Smart Home, Internet of Things, and Connected Cars will present security experts and users with additional challenges in the years to come. Meanwhile, the management of organisations must increasingly address the question of the possible effects of a cyber attack, for example. In addition to one's own organisations, customers, suppliers, and business partners, as well as additional groups may be affected. Therefore, the approach by all those involved must be planned and organised in order to be able to establish and maintain and continuously improve an appropriate and sufficient level of security.

In practice, it often proves difficult to establish and maintain an appropriate and sufficient level of security in the long run. In combination with the increasing complexity of the IT systems, a lack of resources and austerity budgets continuously present the persons in charge with new challenges. Due to the shorter and shorter development cycles, even tried and tested security mechanisms require constant adaptation or even re-design. In the long run, a static solution is not capable of providing an appropriate level of security. However, the common belief that security safeguards would inevitably be associated with high investments in security technology and highly specialised security experts is not true. The most important success factors include common sense, thought-through organisational regulations, and reliable, well-informed employees implementing the security requirements in a self-dependent and experienced manner. Hence, the development and implementation of an efficient security concept does not necessarily have to be unaffordable and the most efficient safeguards may prove surprisingly simple.

Thus, security must be an integral part of planning, design, and operation of business processes and information processing. As a consequence, comprehensive organisational and personnel measures must be taken. Information security management based on IT-Grundschutz includes infrastructural, organisational, and personnel aspects, in addition to technical aspects. Only a holistic approach regarding the increase of information security may affect all levels in a sustainable manner.

An appropriate level of security primarily depends on the systematic approach and only secondarily on the individual technical measures. The following considerations illustrate this hypothesis and the importance of the management level regarding the security process:

- the management level is responsible for ensuring that statutory regulations and contracts with third parties are complied with and that important business processes are not disrupted.
- The management level is the instance making the decisions on how to handle risks.
- Information security has interfaces with many areas of an organisation and affects highly important business processes and tasks. Therefore, only the management level can ensure that information security management is integrated smoothly in existing organisational structures and processes.
- Furthermore, the management level is responsible for the efficient deployment of resources.

Thus, the management level has a high degree of responsibility in the field of information security. A lack of supervision, an unsuitable security strategy, or wrong decisions may have far-reaching negative effects as a result of both security incidents and missed opportunities and bad investments. Involving the management level intensively is absolutely necessary: information security is a top management priority!

This standard therefore describes, in a step-by-step fashion, how successful information security management may be established and which tasks the management level in government agencies and companies will have in this context.

1.3 Addressees

This BSI standard 200-1 is primarily intended for persons in charge of information security, security officers, security experts, security consultants, and all parties interested charged with information security management. Likewise, it forms a reasonable basis for the persons in charge of IT and Industrial Control Systems (ICS), managers and project managers ensuring that the aspects of information security management are adequately taken into account in their organisation and projects.

Efficiently managing information security is not only an important issue for large organisations, but also for small and medium-sized government agencies and companies as well as for the self-employed. The design of an appropriate information security management system depends on the size of the organisation. This standard including the practice-oriented IT-Grundschutz recommendations supports persons in charge wishing to improve the information security in their area of influence. Hereinafter, information will be provided continuously on how the recommendations of this standard can be adapted adequately depending on the size of the organisation.

1.4 Application

The present standard describes how an information security management system (ISMS) can be designed. A management system encompasses all the provisions ensuring the supervision and management so that the organisation can achieve its objectives. An information security management system therefore specifies the instruments and methods that the management level of an organisation should use to comprehensibly manage the tasks and activities aimed at achieving information security.

This BSI standard provides answers to, among other things, the following questions:

- What are the success factors in the field of information security management?
- How can the security process be managed and monitored by the management responsible?
- How are security objectives and an appropriate security strategy developed?
- How are security safeguards selected and security concepts drawn up?
- How can an already achieved level of security be maintained and improved in the long run?

This management standard provides a clear overview of the most important tasks of security management. The BSI provides assistance with implementing these recommendations in the form of the IT-Grundschutz methodology. The IT-Grundschutz provides different sizes and types of organisations with step-by-step guides to developing an information security management in practice and gives specific safeguards for all aspects of information security. The IT-Grundschutz methodology is described in BSI standard 200-2 (see [BSI2]) and is designed in a way that a level of security can be achieved that is appropriate regarding both the basic threat situation and the business objectives. In addition to this, requirements for the practical implementation of the appropriate level of security are formulated in the IT-Grundschutz compendium.

If the term “IT system” is used in this standard, this term shall not only refer to “classical” IT systems such as servers, personal computers, smartphones or network components. Here, the term “IT systems” also includes Industrial Control Systems (ICS) as well as components from the field of Internet of Things (IoT).

2 Introduction to information security

2 Introduction to information security

What is information security?

Information security has the objective of protecting information of any type and origin. In this, information might be stored on paper, in IT systems, or even inside the users' heads. As a subset of information security, IT security focuses on the protection of electronically stored information and its processing.

The classical basic values of information security include confidentiality, integrity, and availability. Many users include additional basic values in their considerations. Depending on the individual use cases, this may be very helpful. Further generic umbrella terms in the field of information security, for example, include authenticity, reliability, reliableness, resilience, and non-repudiation.

Information security is not only threatened by wilful acts (e.g. malware, interception of communications, or computer theft). The following examples illustrate the aforementioned:

- Force majeure (e.g. fires, flooding, storms, and earthquakes) affects data storage media and IT systems or blocks access to the computer centre. Documents, IT systems, or services are no longer available as required.
- After an unsuccessful software update, applications cease to function or data has been modified without this being noticed.
- An important business process is delayed, because the only employees familiar with the software application are ill.
- Confidential information is inadvertently passed on to unauthorised persons by an employee, because documents or files have not been marked "confidential".

Choice of words: IT security versus information security and cyber security

Since the electronic processing of information is omnipresent in virtually all areas of our lives, distinguishing between whether information is processed using information technology, communications technology, or on paper is no longer up-to-date. The term "information security" instead of IT security is therefore more comprehensive and more appropriate. However, it should be noted that the term "IT security" still is frequently used in the literature (among other things, because it is shorter), even if "information security" often is what is meant. The field of action of classical IT security is expanded to the entire cyberspace under the term "cyber security". This term includes the entire information technology connected to the Internet and comparable networks and also includes communications, applications, processes, and processed information based thereon.

2.1 Overview of standards for information security

In the field of information security, many different standards have been developed partially focusing on other target groups or topics. The use of security standards in companies and government agencies does not only improve the level of safety, it additionally facilitates the coordination between different organisations regarding the security safeguards to be implemented in what form. The following overview shows the orientations of the most important standards.

2.1.1 ISO standards on information security

In the international standardisation organisations ISO and IEC, the standards on information security are merged in the continuously growing 2700x series. Internationally, these standards are called standards. These international standards are partly available as translated DIN standards.

The most important standards of the ISO/IEC 2700x series include:

ISO/IEC 27000 (Information security management systems – Overview and vocabulary)

This standard provides an overview of information security management systems (ISMS) and on the correlations of the different standards of the ISO/IEC 2700x family. Furthermore, the standard includes the basic terms and definitions for ISMSs.

ISO/IEC 27001 (Information security management systems – Requirements)

The ISO standard 27001 is an international standard on information security management also allowing for certification. On approx. 9 pages, the ISO/IEC 27001 provides normative specifications regarding the implementation, operation, and enhancement of a documented information security management system. In a normative annex, more than a hundred safeguards (controls) are mentioned that should be selected in consideration of the relevant risks. However, the readers are not provided with any assistance for practical implementation.

Up to now, the requirements of the ISO/IEC 27001 oriented on a lifecycle model also referred to as PDCA cycle according to the names of the different phases (“Plan”, “Do”, “Check”, “Act”). In order to achieve compatibility with annex SL (policy for developing and reviewing ISO standards for management systems), the PDCA cycle is no longer mentioned explicitly in the reviewed version of the ISO/IEC 27001. This is intended to make clear that the sequence of the individual requirements in the standard does not allow to draw any conclusion regarding their respective importance or their implementation sequence. Any activities related to establishing and operating the ISMS can still be performed according to the PDCA cycle, however.

ISO/IEC 27002 (Code of practice for information security controls)

This standard supports in the selection and implementation of the safeguards described in ISO/IEC 27001 in order to establish a working security management and embed it in the organisation. The security safeguards appropriate in this regard are described on the 90 pages of the standard ISO/IEC 27002. The recommendations are primarily intended for the management level and therefore hardly include any technical information. The implementation of the security recommendations of ISO/IEC 27002 is one of many options for fulfilling the requirements of the ISO standard 27001.

ISO/IEC 27004 (Monitoring, measurement, analysis and evaluation)

The ISO standard 27004 addresses the evaluation of the implementation and efficiency of an ISMS based on different variables.

ISO/IEC 27005 (Information security risk management)

This standard includes framework recommendations for information security risk management. Among other things, it supports in the implementation of the recommendations from ISO/IEC 27001. However, no specific risk management method is specified in so doing. This standard in turn is mainly based on the standard ISO/IEC 31000 *Risk management – Principles and guidelines on implementation* (see [31000]). The supporting standard ISO/IEC 31010 *Risk assessment techniques* (see [31010]) includes a description on how risk assessment can be integrated in a risk management system and how risks can be identified, evaluated, assessed, and handled. Annex B of ISO 31010 provides a comprehensive overview of risk assessment methods, 31 different methods are mentioned here.

ISO/IEC 27006 (Requirements for bodies providing audit and certification of information security management systems)

The ISO standard 27006 specifies requirements regarding the accreditation of certification bodies for ISMSs and also addresses specifics of the ISMS certification processes.

ISO/IEC 27009 (Sector-specific application of ISO/IEC 27001 – Requirements)

The ISO standard 27009 describes how sector-specific enhancements (e.g. from the fields of Energy, Cloud Computing, Finances) may be incorporated in an ISMS according to ISO/IEC 27001 in the future and be taken into account as requirements there. For this, individual safeguards from the annex of ISO/IEC 27001 can be enhanced and complemented.

Sector-specific standards (ISO/IEC 27010 – ISO/IEC 27019)

Many sector-specific standards (e.g. ISO/IEC 27019 for the energy industry) are developed based on the ISO/IEC 27009.

Additional standards of the ISO 2700x series

The ISO 2700x series of standards will presumably consist of the ISO standards 27000 – 271xx in the long run. All standards of this series address different security management aspects and refer to the requirements of ISO/IEC 27001. The further standards are intended to provide a better understanding and practical applicability of ISO/IEC 27001. For example, these address the practical implementation of ISO/IEC 27001 and methods regarding the continuity of business processes.

2.1.2 Selected BSI publications and standards on information security

IT-Grundschutz

Since 1994, IT-Grundschutz is the BSI’s methodology for information security. IT-Grundschutz is a holistic approach regarding the implementation of an appropriate information security for organisations of any type and size. With the combination of the IT-Grundschutz approaches for basic, standard and core safeguards, described in BSI-Standard 200-2 *IT-Grundschutz methodology*, and the IT-Grundschutz compendium containing security requirements for the most different deployment environments, IT-Grundschutz offers an efficient and effective tool for selecting and adapting adequate safeguards regarding the safe handling of information for an organisation. Right from the beginning, IT-Grundschutz has been designed to be adapted modularly to different deployment environments by the users. In this regard, the BSI continuously updates and enhances it.

Political framework conditions such as the German IT Security Act, the very dynamic topic of information security, as well as the increasingly more professional cyber attacks tipped the balance to a fundamental re-modernisation of the IT-Grundschutz. With the present BSI standards 200-1 to 200-3, this resulted in additional approaches allowing for gradually getting started regarding a security management. These are complemented by IT-Grundschutz modules summarised in the IT-Grundschutz compendium. Figure 1 illustrates the structure of the IT-Grundschutz documents.

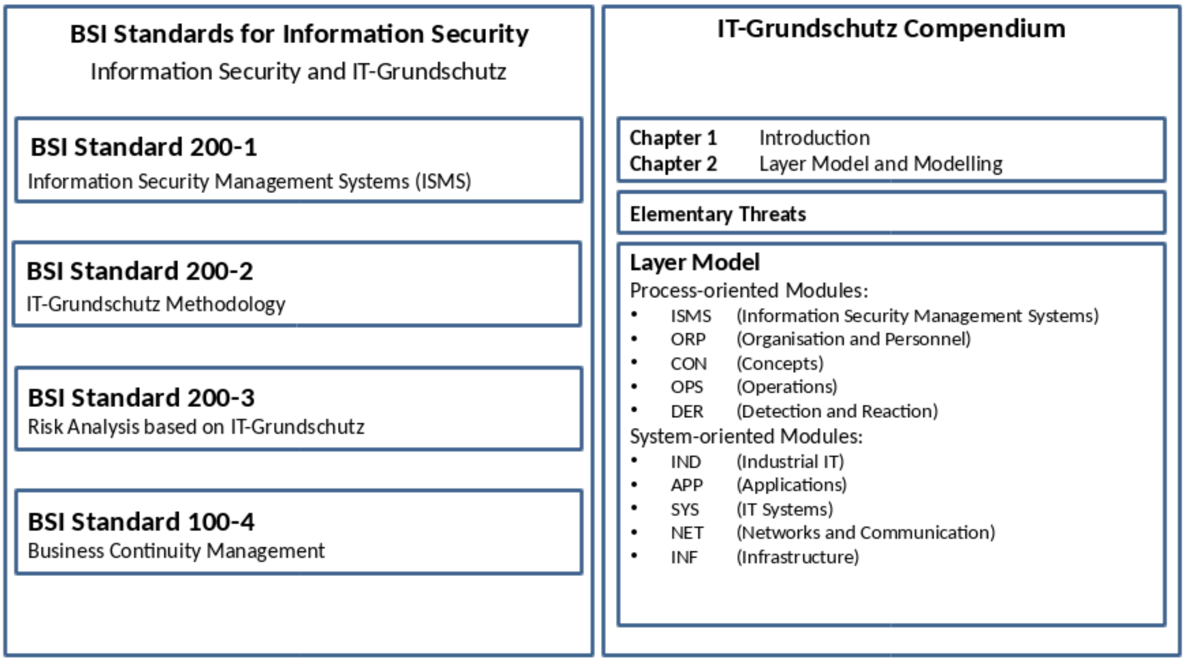

BSI Standards for Information Security
Information Security and IT-Grundschutz
BSI Standard 200-1
Information Security Management Systems (ISMS)
BSI Standard 200-2
IT-Grundschutz Methodology
BSI Standard 200-3
Risk Analysis based on IT-Grundschutz
BSI Standard 100-4
Business Continuity Management
IT-Grundschutz Compendium
Chapter 1 Introduction
Chapter 2 Layer Model and Modelling
Elementary Threats
Layer Model
Process-oriented Modules:
• ISMS (Information Security Management Systems)
• ORP (Organisation and Personnel)
• CON (Concepts)
• OPS (Operations)
• DER (Detection and Reaction)
System-oriented Modules:
• IND (Industrial IT)
• APP (Applications)
• SYS (IT Systems)
• NET (Networks and Communication)
• INF (Infrastructure)

Figure 1: Overview of BSI publications on security management

The IT-Grundschutz compendium has a modular design and includes process and system modules for typical business processes, applications, systems, communication connections, and rooms. The modules applicable to the framework conditions of one's own organisation can be used as required. IT-Grundschutz addresses all areas that may be found in organisations. Along with organisation and personnel, this also includes IT operations, but also production and manufacture using Industrial Control Systems (ICS), as well as components from the field of Internet of Things (IoT).

Every module includes a short description of the topic and the objective that is to be achieved by implementing the module, as well as a delimitation regarding other modules related regarding the topic. Furthermore, there is an overview of the specific threats of the topic under consideration. The security requirements for the basic, standard, and core safeguards form the core of every module.

Additionally, there may be implementation recommendations for the modules of the IT-Grundschutz compendium. These describe how the requirements of the modules can be satisfied in practice and include appropriate security safeguards including detailed descriptions that are based on the wealth of experience and best practices of BSI and IT-Grundschutz users.

The modules of the IT-Grundschutz compendium and the implementation recommendations are updated and expanded at regular intervals. Therefore, they are published as a printed version and additionally on the Internet for free.

Series of BSI standards on information security: Topic IS management

200-1 Information security management systems (ISMS)

The present standard defines general requirements for an ISMS. Therein, it is described which safeguards can be used to generally initiate, control, and monitor information security in an organisation. The BSI standard 200-1 is completely compatible with the ISO/IEC 27001 standard and furthermore takes into account the terms defined in ISO standard ISO/IEC 27000 as well as the recommendations in ISO standard ISO/IEC 27002. It provides readers with an easy to understand and systematic guide irrespective of which method an organisation wants to use in order to implement the requirements for an ISMS.

The BSI renders the content of the ISO standards mentioned above in its own BSI standard in order to be able to describe some topics in greater detail and thus allow for a didactically improved representation of the content. Furthermore, the structure has been designed in such a way that it is compatible with the IT-Grundschutz methodology.

200-2 IT-Grundschutz methodology

The IT-Grundschutz methodology explains, in a step-by-step fashion, how an information security management system can be established and operated in practice. The information security management tasks and the design of an organisational structure for information security are important topics in this regard. The IT-Grundschutz methodology goes into great detail on how a security policy can be developed in practice, how appropriate security requirements can be selected, and what should be considered when implementing the security policy. It also answers the question of how to maintain and improve information security during routine operation.

In order to allow for gradually getting started regarding security management, different methodologies are offered depending on the level of security aimed at and the information to be secured. Depending on which information security methodologies are already present within the organisation, it may be expedient to initially deviate from the "complete" IT-Grundschutz methodology ("standard safeguards"). For example, an organisation may aim at initially implementing all basic requirements ("basic safeguards") as comprehensively as possible in order to reduce the major risks as quickly as possible, before the actual security requirements are analysed in detail. Another thinkable methodology is to initially focus on protecting the essential values of the organisation ("core safeguards").

Based on the BSI standard 200-2, IT-Grundschutz interprets the general requirements and security safeguards of the above-mentioned ISO standards 27001 and 27002 and supports the users regarding the practical implementation by providing comprehensive information, background information, and examples. The modules of the IT-Grundschutz compendium explain what should be done; the implementation recommendations provide very specific information as to how a requirement (also on a technical level) can be fulfilled. Thus, proceeding according to IT Grundschutz is a proven and efficient option of fulfilling all requirements of the above-mentioned ISO standards.

200-3 Risk analysis on the basis of IT-Grundschutz

The BSI has worked out a methodology for risk analysis on the basis of IT-Grundschutz. The BSI standard 200-3 describes how, based on the IT-Grundschutz methodology, a simplified analysis of risks for information processing can be carried out. This is based on the elementary threats described in the IT-Grundschutz compendium and also forming the basis for drawing up the IT-Grundschutz modules. This methodology can be used when companies or government agencies are already working successfully with IT-Grundschutz and would like to add a risk analysis to the IT-Grundschutz analysis as seamlessly as possible.

100-4 Business continuity management

In the BSI standard 100-4, a methodology for establishing and maintaining an agency- or company-wide business continuity management is explained. In this, the methodology described herein builds upon the IT-Grundschutz methodology "standard safeguards" described in BSI standard 200-2 and reasonably complements this methodology.

Information security revision policy based on IT-Grundschutz

Information security revision (IS revision) is a part of every successful information security management. Only by regularly reviewing the established security safeguards and the information security process is it possible to make statements regarding their efficient implementation, up-to-dateness, completeness, and appropriateness, and thereby regarding the current status of information security. Hence, the IS revision is a tool for determining, achieving, and maintaining an appropriate level of security within an organisation. In this regard, the BSI developed a method by means of the *IS revision policy based on IT-Grundschutz* (see [BSIR]) that is designed to determine the information security status in an organisation and to be able to identify vulnerabilities.

2.1.3 Additional standards

COBIT 5 A Business Framework for the Governance and Management of Enterprise IT

COBIT 5 considers IT to be the essential basis of an organisation regarding the achievement of the business objectives and requires that the business strategy objectives are incorporated in the IT objectives and that the services provided meet the quality requirements of the business processes. Like ITIL, COBIT 5 relies on targeted, optimised IT processes. COBIT 5 introduces the process potential aspect, addressing the extent to which an organisation is able to achieve the required objectives in a reliable and sustainable manner. The overview of the maturity of all 37 process areas, grouped into five domains, can be used to derive the professionalism of the supporting IT processes. The COBIT documents are published by the Information Systems Audit and Control Association (ISACA). When drawing up COBIT, the authors oriented on existing standards regarding the topic of security management, particularly ISO/IEC 27002.

ITIL

The IT Infrastructure Library (ITIL) is a collection of several books on the topic of IT-Service-Management. It was developed by the British Office of Government Commerce (OGC). ITIL addresses the management of IT services from the IT service provider's point of view. In this, the IT service provider may be both an internal IT department and an external service provider. The overall objective is to optimise and improve the quality of IT services and the cost efficiency. Information security is considered from the operative perspective within the framework of the considered services. By the same token, working IT operations are an essential buttress for the ISMS, which is why many disciplines of ITIL can be found similarly in IT-Grundschutz and other security standards, but with the focus on information security.

Based on ITIL, the standard ISO/IEC 20000 was drawn up that can be used as the basis for certifying a service management system.

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is published by a consortium of leading credit card organisations. It was drawn up by the PCI Security Standards Council and formulates security requirements regarding the processing of credit card transactions. The requirements of PCI DSS must be implemented by all organisations storing, processing, or transmitting card holder data of credit cards, e.g. by dealers accepting credit card payments or by service providers further processing these by order.

NIST

The U.S. National Institute of Standards and Technology (NIST) is a federal agency responsible for developing standards, among other things. These standards are binding for U.S. government agencies. In the series *Special Publication 800* (NIST SP 800 series), the NIST regularly publishes documents on individual information security topics (cryptography, cloud computing, etc.) not only providing valuable information, but also having comprehensive international influence on the design of information security.

In this, the document NIST SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* summarises a large number of so-called controls for the field of security management that may be used in order to protect information clusters. The controls are grouped into diverse areas according to topics belonging together (e.g. training and awareness-raising measures, authorisation management, infrastructure security).

ISF – The Standard of Good Practice

The Information Security Forum (ISF) is an independent and globally active organisation for information security. With the *Standard of Good Practice* (SoGP), the ISF publishes an information security policy based on recognised "best practices". According to their own statements, the practice-oriented policy covers the requirements of the standards ISO/IEC 27002, COBIT 5, PCI DSS 3.1 and

NIST Cybersecurity Framework. The SoGP groups the different topics into diverse areas (e.g. security governance, information risk assessment).

3 ISMS definition and process description

3.1 Components of an information security management system

On the one hand, the term management refers to the management level, i.e. the entirety of the managers of an organisation, and, on the other hand, it generally also refers to the task of managing the organisation. For the purpose of differentiation, the group of responsible managers shall hereinafter be referred to as “management level”, when referring to the responsible managers and when there is a risk of confusion with the term “management” as an activity (supervising, directing, and planning).

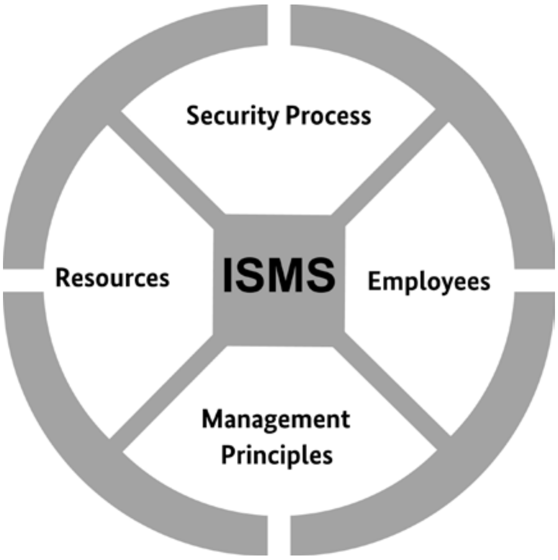


Figure 2: Components of an information security management system (ISMS)

A management system embraces all the policies pertaining to supervision and management for the purpose of achieving the organisation’s objectives. The part of the management system dealing with information security is referred to as the information security management system (ISMS). The ISMS specifies the instruments and methods that the management level should use to clearly manage (plan, adopt, implement, supervise and improve) the tasks and activities aimed at achieving information security. ISMS involves the following essential components (see Figure 2):

- management principles
- resources
- employees
- security process
    - information security policy which the security objectives and strategies for their implementation are documented in
    - security concept
    - security organisation

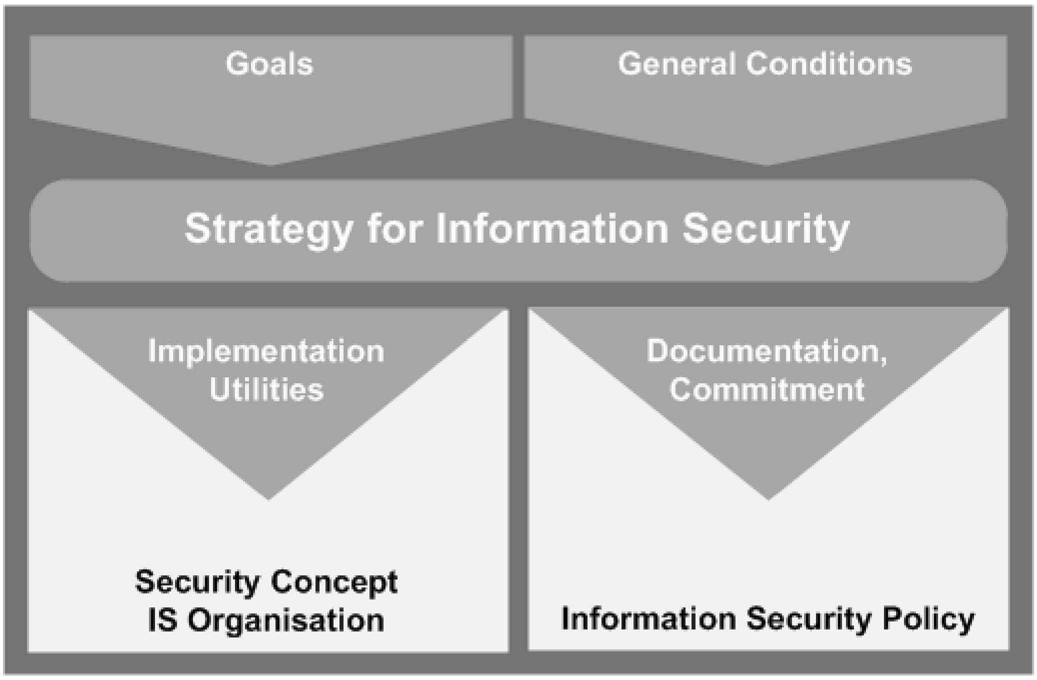

Goals
General Conditions
Strategy for Information Security
Implementation Utilities
Documentation, Commitment
Security Concept
IS Organisation
Information Security Policy

Figure 3: Information security strategy as a central component of the ISMS

The security strategy serves for orientation for planning the next steps in order to achieve the security objectives set. The strategy is specified by the management level and is based on the company's business objectives or the government agency's role. In this, security policy and security concept are the tools of the management regarding the implementation of the security strategy.

Figure 3 and Figure 4 illustrate this interrelationship more clearly. The central points of the security strategy are documented in the information security policy. The security policy is of primary importance, since it contains a visual record of the management level's commitment to its strategy.

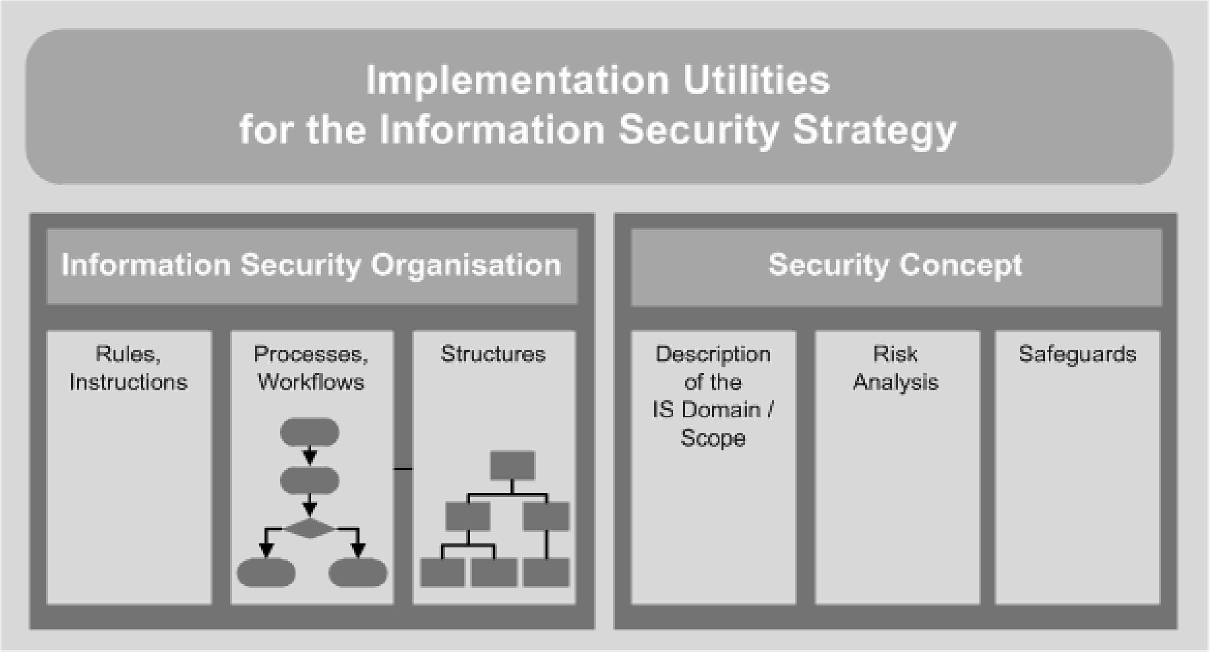


Figure 4: Implementation of the security strategy with the help of the security concept and an information security organisation

3.2 Process description and lifecycle model

3.2.1 The lifecycle in information security

Security is not a permanent state which, once achieved, will never change. Every organisation is subject to constant change. Many of these changes also affect information security, along with changes in the business processes, specialised tasks, infrastructure, organisational structures and the IT. Besides the obvious changes within an organisation, changes to external framework conditions may also occur, for example, the statutory or contractual stipulations as well as the available information and communications technologies might change considerably. Due to new attack methods or vulnerabilities, security concepts and safeguards may partially or completely become inefficient. It is therefore necessary to actively manage information security so that the level of security that has been reached can be maintained and improved on a continuous basis.

It is not sufficient, for instance, to plan the implementation of business processes or the introduction of a new IT system just once and then implement the agreed security safeguards. After security safeguards have been implemented, they must be examined regularly to ensure they are effective, appropriate, applicable, and also actually being applied. If vulnerabilities or opportunities for improvements are discovered, the safeguards must be adapted and improved. The necessary adaptations and changes again require planning and implementation. If business processes are terminated or components and IT systems are replaced or shut down, security aspects must also be considered in so doing (e.g. the withdrawal of authorisations or the secure deletion of hard drives). As a consequence, the security safeguards are grouped into the following phases for a clearer overview in the implementation recommendations regarding the modules of the IT-Grundschutz compendium:

- planning and design,
- purchasing (if necessary),
- implementation,
- operation (measures for maintaining information security during normal operation including monitoring and performance review),
- discharge (if required), and
- contingency planning.

3.2.2 Description of the information security process

Such a “lifecycle” does not only apply to business processes and IT systems. A security strategy, a security concept, a security organisation, and ultimately the entire security process are subject to a lifecycle. In order to describe the dynamics of the security process as simply as possible, it is frequently divided into the following phases in the literature:

1. planning,
2. implementing the plan and carrying out the project,
3. performance review and/or monitoring the achievement of objectives, and
4. eliminating discovered flaws and vulnerabilities and making optimisations and improvements.

Phase 4 describes the immediate elimination of minor flaws. If fundamental or extensive changes are needed, one must of course return to the planning phase again.

This model is named after the individual phases (“Plan”, “Do”, “Check”, “Act”) and is thus also referred to as the PDCA cycle.

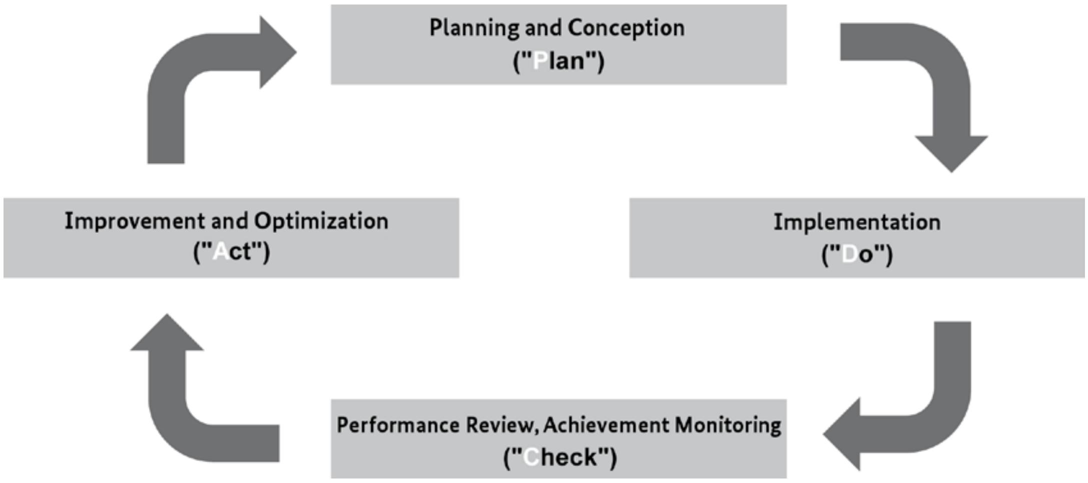

Planning and Conception
("Plan")
Implementation
("Do")
Performance Review, Achievement Monitoring
("Check")
Improvement and Optimization
("Act")

Figure 5: Lifecycle according to Deming (PDCA cycle)

As a matter of principle, the PDCA cycle can be applied to all tasks within the security process. The lifecycle of the security concept and the security organisation can also be described clearly using this cycle. The relevant chapters in this document therefore use the four phases of this lifecycle model as their basis.

During the planning phase of the security process, the framework conditions are identified and analysed, the security objectives are determined, and a security strategy is drawn up containing the basic statements on how the set objectives should be achieved. The security strategy is implemented with the help of the security concept and an appropriate security organisation structure. Security concept and organisation require planning, implementation, and a performance review. The performance review of the superior security process involves regularly examining whether the framework conditions (e.g. laws, objectives of the organisation, or the environment) have changed and whether the security concept and organisation have proven to be effective and efficient.

However, since different organisations have different initial conditions, security requirements, and financial resources, this methodology serves as a sound basis for orientation, but must be adapted to the specific needs by every government agency and company. Each organisation must define and specify individually the form of the lifecycle model that is appropriate for them.

Small government agencies and companies should not be put off by this, since the effort required for the security process generally depends on the size of the organisation. In a very large company with many departments and individuals involved it is therefore probably necessary to implement a rather formal process precisely defining what internal and external audits are needed, who should report to whom, who should draw up decision papers, and when the management should meet to discuss the security process. In a small company, on the other hand, an annual meeting between the managing director and the IT service provider, within the framework of which they discuss the problems experienced throughout the past year, the costs incurred, the latest technological developments, and other factors, might already be sufficient in order to critically examine the success of the security process.

4 Management principles

Information security management or abbreviated IS management is the term referring to the planning and supervisory functions that are required to assure the meaningful development, practical feasibility, and effectiveness of a well thought-through and systematic security process as well as all the security safeguards required for this. This also includes the processes of meeting and complying with statutory and regulatory requirements. There are various concepts as to what an efficient IS management may look like and which organisational structures are expedient in this regard. Regardless of the form an IS management system takes, there are several principles that must be considered.

Some of the management principles presented here might sound somewhat trivial, since most managers will consider them a matter of course. Paradoxically, however, it is precisely the simple things that are put into practice incorrectly or omitted completely. Although discipline, patience, the ability to take on responsibility, and preparation of projects in a realistic and careful manner are recognised values in many organisations in theory, they are not always put into practice. Particularly the less spectacular safeguards, such as process optimisation, training and awareness-raising measures, as well as staff motivation, or the drawing up of comprehensible documentation, are the ones that improve the level of security in practice quite substantially. Complex and therefore expensive safeguards, large-scale projects, and investments in technology are frequently very wrongly portrayed as being more effective and frequently are responsible for the poor reputation of security safeguards as a cost driver. In the following, we shall therefore present management principles which, when observed, form a good basis for successful information security management.

4.1 The tasks and duties of management

The tasks and duties of the management level with regard to information security can be summarised in the following items:

1. Assumption of overall responsibility for information security

The topmost management level of every government agency and company is responsible for the organisation working in a targeted and proper manner and is therefore also responsible for assuring information security both on the inside and out. Depending on the country and type of organisation, this can also be governed by various laws. The management level, but also every individual manager, must clearly demonstrate their commitment to their responsibility and must explain the importance of information security to all employees.

2. Initiating, managing, and supervising information security

The topmost management level must initiate, manage and supervise the security process. This, for example, involves the following tasks:

- A strategy for information security and security objectives must be agreed upon and communicated. The security strategy is based on the business objectives of the company or the role of the government agency.
- The impact of security risks on the business operation or on the fulfilment of tasks must be investigated. The management level is the instance making the decisions on how to handle risks. The responsibility for information security remains there. However, the operative task “information security” is typically delegated to an information security officer (ISO).
- The organisational framework conditions for information security must be created, responsibilities and authorisations must be assigned and communicated.
- Sufficient resources must be made available for information security. The security strategy must comply with the resources that are available.
- The security strategy must be reviewed and assessed at regular intervals, e.g. the achievement of the objectives can be monitored with the help of key figures. Identified vulnerabilities and

errors must be corrected. For this, an “innovative” working atmosphere must be created and the will for constant improvement must be demonstrated within the organisation.

- Employees must be motivated regarding security issues and must consider information security an important aspect of their tasks. For this, appropriate training and awareness-raising measures must be offered, among other things.

3. Integration of information security

Information security is a cross-sectional function and must therefore be integrated in all processes and projects of the organisation processing information. Examples of this include:

- project management: already in the planning phase of a project, the protection requirements of the information to be processed in the future as a result must be assessed and, building thereon, suitable security safeguards must be planned.
- incident management: in the event of failures of the IT operations having effects on the information security, the approach must be coordinated with the security management. The security incident management and failure management of the IT and the facility management departments must be interconnected.

If such management processes do not exist, it is possible to establish and operate an ISMS, but it will not work efficiently. If ISMS and project management are not interconnected, the protection requirements of new or changed business processes may only be determined by cyclic samples (annually, quarterly). As a consequence, it is significantly more difficult to obtain a complete and up-to-date determination of protection requirements of all the target objects. If no fault management is present, security incidents will not be detected and/or not reported to the correct body. The degree of maturity of information security therefore also depends on the degree of maturity of the other management processes of the organisation and is not an independent variable.

4. Setting objectives that can be achieved

Projects frequently fail because the objectives that have been set are unrealistic or too ambitious. This is no different in the field of information security. In order to achieve the reasonable security objective, many small steps and a long-term, continuous process of improvement without high investment costs may, in the beginning, be more efficient than a large-scale project. This way, it may be expedient to initially implement the necessary level of security within selected areas only, and, for instance, using the basic safeguards from IT-Grundschutz regarding the width or the core safeguards IT-Grundschutz regarding the depth there. However, using these nuclei as starting points, the security in the organisation must then be increased quickly to the level aimed at.

5. Pondering security costs against benefits

One of the most difficult tasks is to ponder the costs for information security against the benefits and risks. It is very important to initially invest in safeguards that are particularly effective or provide protection against especially high risks. Experience shows that the most effective safeguards are not always the most expensive ones. It is therefore absolutely necessary to understand the dependence of the business processes and tasks on information processing so that appropriate safeguards can be selected.

At this point, it should be emphasised that information security is only ever achieved by interaction between technical and organisational safeguards. The investments in technology can be read off the budget directly. In order to justify these costs, the security products must be deployed in such a manner that they are of maximum benefit. The products must therefore have been selected for the purpose that they should serve and must be operated in the appropriate manner, i.e. they must be integrated in the holistic security concept and employees must be trained in how to use them. Technical solutions can frequently be replaced by organisational security safeguards. However, experience has shown that it is more difficult to ensure that organisational safeguards are implemented consistently. Furthermore, doing so requires more personnel and thus also places a burden on the resources.

6. Role model function

The management level must assume a role model function also when it comes to information security. Among other things, this includes that the management level takes into account all specified security rules, participates in training measures, and supports other managers regarding the execution of their role model function.

4.2 Communication and knowledge

Communication is an important cornerstone regarding the achievement of the set security objectives in all phases of the security process. Misunderstandings and lack of knowledge are the most common causes for security issues. A smooth flow of information regarding security incidents and security safeguards must therefore be assured on all levels and in all departments of an organisation. This involves the following items:

- **Reports to the management level**

  The management must ensure it is kept up-to-date about problems, the results of reviews and audits, but also the latest developments, altered framework conditions, or opportunities for improvement at regular intervals so that it can fulfil its management function. In order for the management level to be able to make the right decisions regarding the control and management of the information security process, they need basic information relating to the information security status. This basic information should be prepared in management reports and reported regularly by the ISB to the management level in an appropriate form. The management level acknowledges the management reports and possibly prompts required safeguards.

- **Flow of information**

  Inadequate communication and a lack of information may lead to security issues, but also to incorrect decisions or unnecessary working steps. This must be avoided by personnel safeguards and organisational regulations. Employees must be informed about the purpose of security safeguards, particularly if these safeguards cause additional work or result in reduced convenience. Furthermore, employees should be informed on the legal issues of information security related to their work, as well as on data privacy. Moreover, employees should be involved in the implementation planning of safeguards so that their ideas are also considered and they are given the opportunity to assess the practical feasibility of these safeguards.

- **Classification of information**

  In order to be able to appropriately protect information, their importance for the organisation must be clear. In order to easier exchange information on the value of certain types of information within an organisation, but also with other organisations, a classification scheme is necessary describing the available stages of importance and how the different stages are delimited against each other.

- **Documentation**

  To ensure the continuity and consistency of the entire security process, it is absolutely necessary to document the process. This is the only manner of ensuring that the various process steps and decisions remain comprehensible. Furthermore, meaningful documentation ensures that similar tasks are performed in the same manner, i.e. processes therefore become measurable and repeatable. Documentation also aids in recognising fundamental vulnerabilities in the process and in avoiding the repetition of errors. The documentation necessary for the various security activities fulfils different functions and is intended for different target groups. The following documentation types can be differentiated:

  1. Technical documentation and documentation for work processes (target group: experts)

     During failures or security incidents it must be possible to restore the desired target status of the business processes and the related IT. Technical details and workflows must therefore be documented in such a way that this can be achieved within a reasonable amount of time.

Examples of this are instructions for installing IT applications, for performing data backups, for restoring data backups, for configuring the PBX, for restarting an application server after a power failure, as well as the documentation for testing and approval procedures and instructions on what to do when failures and security incidents occur.

Work procedures, organisational stipulations, and technical security safeguards must be documented such that security incidents caused by a lack of knowledge or mistakes can be avoided. Examples of this include security policies for the use of email and the Internet, information on how to prevent infection by viruses or on how to recognise social engineering, as well as rules of conduct for employees if they suspect a security incident has occurred.

2. Management reports (target group: management level, security management)

   All the information the management requires in order to be able to fulfil its management and supervisory duties must be recorded with the required level of detail (e.g. results of audits, measurements of effectiveness, reports on security incidents).

3. Records of management decisions (target group: management level)

   The management level must record and justify the selected security strategy. Furthermore, decisions affecting aspects relevant to security that are taken on all the other levels must also be recorded to ensure they can be comprehended and repeated at any time.

Therefore, in the following chapters, every action that must be suitably documented or recorded is indicated with “[DOC]”.

- **Formal requirements for documentation:**

  Documentation does not necessarily have to be available in paper form. The documentation medium should be selected as required. For example, the use of a software tool might be helpful for business continuity management that can be used to previously capture all business continuity safeguards and contacts and in a mobile manner in the event of a crisis. This tool, all necessary information, and the required IT systems must be available in cases of emergency, e.g. on a laptop. Depending on the emergency, it may make more sense to have all information at hand in a practical printed manual.

  There may be statutory or contractual requirements regarding the documentation that must be observed, e.g. storage periods and levels of detail. Documentations only fulfil their purpose if they are drawn up and updated at regular intervals. Furthermore, the documentation must be identified and stored in such a way that it can be used when necessary. It must be clearly visible who drew up which parts of the documentation and when these parts were drawn up. If references are made to other documents, the relevant sources must be described. Additional documents must also be available if required, furthermore.

  Security-relevant documentation may contain information requiring protection and must therefore be suitably protected. Along with the protection requirements, the type and the duration of storage and options for the destruction of information must be defined. The process descriptions must describe whether and how the documentation must be evaluated, who must edit the documentation at which intervals, and who will have access rights to it.

- **Utilising available sources of information and experiences**

  Information security is a complex issue, so the persons responsible for it must familiarise themselves with it very carefully. There are many sources of information available that can be used in this regard. These include, among other things, existing standards, Internet publications, and other publications. Furthermore, the cooperation with associations, partners, committees, and other companies or government agencies as well as CERTs (Computer Emergency Response Teams) should be used for exchanging experiences about successful security activities. Since the subject of information security is very broad, it is important to identify and document the sources of information and cooperation partners that are appropriate for the respective organisation and the framework conditions.

4.3 Performance review within the security process

The management level must regularly check the performance and assess the security process (management assessment). If required (e.g. if a number of security incidents occur or there are significant changes to the framework conditions), corresponding audits and assessments must be performed between the regular dates. All results and decisions must be documented in a comprehensible manner [DOC].

The following questions, among other things, should be addressed during the discussion:

- Have framework conditions changed resulting in the need to change the approach regarding information security?
- Are the security objectives still appropriate?
- Is the information security policy still up-to-date?

In this, the focus of the performance review regarding the security process is not on auditing individual security safeguards or organisational regulations, but on assessing the situation as a whole. For example, the secure operation of an Internet portal might turn out to be too expensive for a small company. The management level could then, as an alternative, charge a service provider with the administration of the portal.

In this situation, it is useful to examine how the security concept and the security organisation have performed to date. In chapter 8 *Security concept*, various activities are described for reviewing the performance of individual security safeguards. The results gathered there should be taken into account when reviewing the performance of the security strategy. If, for example, it turns out that the security safeguards are ineffective or decidedly expensive, this might give reason to reconsider and adapt the entire security strategy. The following questions should be addressed:

- Is the security strategy still appropriate?
- Is the security concept appropriate for achieving the set objectives? Are, for instance, the legal requirements fulfilled?
- Is the security organisation appropriate for achieving the objectives? Should its position within in the organisation be strengthened or should it be integrated more in the internal processes?
- Is there an appropriate relation between the effort – i.e. costs, personnel, materials – required to achieve the security objectives and the business objectives and the role of the organisation?

4.4 Continuous improvement of the security process

The results of the performance review must be used consistently to make appropriate corrections. This might mean that the security objectives, the security strategy, or the security concept must be changed and the security organisation must be adapted to the requirements. It may make sense to subject the business processes and the IT environment to fundamental changes or to discontinue or outsource business processes if, for instance, their secure operation cannot be guaranteed using the available resources. If major changes are required and more comprehensive improvements must be implemented, this will result in a return to the planning phase, thus completing the management cycle.

5 Resources for information security

Maintaining a particular level of security always requires financial, personnel, and time-related resources that must be made available in sufficient quantities by the management level. If set objectives cannot be achieved due to a lack of resources, it is not the fault of the persons responsible for the implementation, but rather the fault of the superiors who have set unrealistic objectives or have not provided the necessary resources. In order to fulfil the set objectives, it is important that an initial cost-benefit estimation is performed already when the objectives are defined. In the course of the security process, this aspect should continue to play a decisive role so that, on the one hand, resources are not wasted, and, on the other, the investments necessary for achieving an appropriate level of security are guaranteed.

Frequently, only technical solutions are associated with IT security. However, this is too short-sighted. This is another reason for better using the term information security instead of IT security. First and foremost, it is important to emphasise that investing in human resources is often more effective than investing in security technology. Technology alone does not solve any problems; it must always be integrated in the organisational framework conditions. The examination of the effectiveness and appropriateness of security safeguards must also be ensured by providing sufficient resources.

In practice, the internal security experts frequently do not have enough time to analyse all the influencing factors and framework conditions that are relevant to security (e.g. statutory requirements or technical questions). To some extent, they lack the relevant basic principles. It always makes sense to consult external experts if questions and issues cannot be clarified or solved using one’s own means. This must be documented by the internal security experts so that the management level provides the necessary resources.

A prerequisite for secure IT operations is a company that functions well. Sufficient resources must therefore be made available for operations. Typical problems encountered during IT operations (scarce resources, overburdened administrators, or an unstructured and poorly maintained IT environment) must generally be solved so that the actual security safeguards can be implemented effectively and efficiently.

6 Involving employees in the security process

Information security affects all employees without any exceptions. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Raising the awareness for information security and providing appropriate training measures for employees as well as for all managers therefore are fundamental prerequisites for information security. In order to be able to implement security safeguards as planned, employees must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves knowledge of the purpose of security safeguards. The working atmosphere, common moral values, and the commitment of employees are all factors decisively influencing information security.

If new employees are employed or existing ones are given new tasks they must be provided with thorough training so they adjust to the new situation. This must also involve teaching them about the security-related aspects of the respective job. If employees leave the organisation or their responsibilities change, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards).

Employees must be obliged to comply with all laws, regulations, and ordinances relevant in the respective environment. For this, they must, of course, be familiarised with the existing information security regulations and simultaneously they must be motivated to comply with these. Moreover, the employees should know that every identified (or suspected) security incident must be reported to security management and how and to whom the report has to be performed.

7 The security process

The management level must define the security objectives knowing all of the relevant framework conditions, the environmental analysis, and based on the business objectives of the company or the role of the government agency and must create the prerequisites for their implementation. The approach is planned with a security strategy to establish a continuous security process. The strategy is implemented with the help of a security concept and a security organisation. In the following, we shall therefore describe the relevant management activities for each lifecycle phase. Due to the broad range and the better overview, the activities relevant to the security concept will be described in a separate chapter.

7.1 Planning of the security process

Determining the framework conditions

The creation of information security is not an end in itself, but information security contributes to the objectives of an organisation being achieved and being able to reliably execute business processes and tasks. For this, it is required that the organisation identifies and analyses all framework conditions, defines the security objectives, and draws up a security strategy containing basic statements on how the set objectives should be achieved. Identifying the framework conditions also includes the analysis of the environment, within the framework of which both internal and external parties, as well as their security requirements, their requirements regarding the ISMS, and their statutory and regulatory requirements are taken into account.

Determining framework conditions is an essential basis for the further considerations regarding information security, since it can be identified where important background information is missing in order to be able to properly assess the importance of information security for the organisation. Furthermore, a first self-assessment is allowed for thereby, since it becomes clear already when compiling the background information where there are potential conflicts and where actions need to be taken.

Formulating security objectives and an information security policy [DOC]

The information security objectives should be determined carefully at the beginning of each security process. Otherwise, there is a risk that the security strategies and concepts drawn out will not match the actual requirements of the organisation.

Thus, the basic objectives of the organisation and the general framework conditions should be used to initially derive general security objectives and make strategic specifications as to how these security objectives should be achieved. The following subjects should at least be considered when developing the security strategy:

- objectives of the company or roles of the government agency
- legal requirements and regulations such as regarding data privacy,
- customer requirements and existing contracts,
- internal framework conditions (e.g. pan-organisation risk management), analysis of the environment,
- (IT-assisted) business processes and specialised tasks, and
- global basic threats to the business activities through security risks (e.g. damage to the image, violations of laws, infringement of contractual obligations, and theft of research results).

The central points of the security strategy are documented in the information security policy. The information security policy should at least contain statements on the following issues:

- importance of information security and the essential information, business processes, and IT for the fulfilment of the tasks,
- reference of the information security objectives to the business objectives or tasks of the organisation,
- security objectives and the key elements of the security strategy for the business processes and the IT used,
- assurance that the security policy is implemented by the management of the organisation, as well as key statements on the performance review, and
- description of the organisational structure established for implementing the information security process.

In addition, the following statements may be added:

- For motivational reasons, some threats that are important to the business processes may be sketched and the most important statutory regulations and other important framework conditions (such as contractual agreements) may be stated.
- The essential tasks and responsibilities within the security process should be illustrated (particularly for the IS management team, the ISO, the employees, and the IT operations, more detailed information on the individual roles can be found in chapter 4 *Organisation of the security process* of BSI standard 200-2 *IT-Grundschutz methodology*. Furthermore, the organisational units or roles should be identified that act as contact persons for security questions.
- Programmes to promote information security via training and awareness-raising measures may be announced.

Determination of the appropriate level of safety of the business processes

In order to better understand the information security objectives, the desired level of security can be described for individual business processes or organisational areas of particular interest with reference to the basic values of information security (confidentiality, integrity, availability). This is helpful for formulating the detailed security concept at a later point in time.

Definition of the scope [DOC]

The scope within which the ISMS should be responsible must be defined initially. The scope frequently includes the entire organisation, but can also, for example, refer to one or more specialised tasks or business processes or one or more organisational units. In this, it is important that the considered specialised tasks and business processes are completely contained within the selected scope and are concluded regarding the content, i.e. no essential parts of any of the business processes are not covered by the scope. Within the context of IT-Grundschutz, the term “information network” is used for the scope. The information network also includes all the infrastructural, organisational, personnel, and technical components that serve to fulfil the tasks in this area of application of information processing.

While the scope frequently comprises the entire organisation regarding the basic and standard safeguards, for the core safeguards the focus is on a few extraordinary, particularly business-critical assets (so-called crown jewels).

7.2 Establishing a security organisation [DOC]

Planning and executing a security process includes defining organisational structures (e.g. departments, groups, centres of expertise) as well as roles and duties. There are different options for organising the structure of information security management. In this, staff arrangements depend on the size of the respective organisation, the existing resources, and the desired level of security. The process of scheduling the resources for supporting information security must be performed such that the agreed level of security can actually be achieved.

When defining roles within the framework of information management, the following basic rules must be observed:

1. The overall responsibility for information security remains with the management level.
2. At least one person has to be appointed who promotes and coordinates the information security process, typically as information security officer (ISO).
3. Every employee is equally responsible for their original task and for maintaining information security at his/her workplace and in his/her environment.

In order to secure direct access to the organisation’s management, the role of the ISO should be organised as an executive department. At management level, the information security role should be clearly assigned to one responsible manager whom the ISO directly reports to.

7.3 Implementation of the information security policy

A security concept must be drawn up in order to achieve the set security objectives. For greater clarity, a separate chapter has been provided to explain how a security concept can be planned and implemented and how the level of information security can be maintained and improved. The results of the check of the security safeguards are then integrated in the performance review of the security process and are assessed by the management level.

7.4 Maintaining information security

Establishing information security is not a project with a limited time span, but a continuous process. The appropriateness and effectiveness of all elements of the information security management system must be checked at regular intervals. This means that not only individual security safeguards must be checked, but also that the security strategy must be reviewed on a regular basis.

The implementation of the security safeguards should be evaluated at regular intervals by means of internal audits. These also serve the purpose of collecting and evaluating the experiences made in day-to-day practice. In addition to audits, it is also necessary to perform drills and awareness-raising measures, since this is the only manner of determining whether all the specified procedures and the conduct in cases of emergency will actually have the desired effect. Findings regarding vulnerabilities and opportunities for improvements must lead to consequences within the security organisation without any exception. Moreover, it is important that future developments both regarding the technology used and the business processes and organisational structures are perceived at an early stage so that potential threats can be identified in time, provisions can be made and security safeguards can be implemented. If significant changes in business processes or organisational structures are looming, the information security management must become involved here. The ISO must become active in a proactive manner: Even if the involvement of the information security management is already planned for in the organisation’s regulations, it should not wait to become involved as planned, but should become involved in the relevant processes of its own accord in good time.

It is important that none of the audits are carried out by those individuals who were involved in the planning and design of the security objectives, because it is difficult to find one’s own mistakes. Depending on the size of the organisation it might be useful to consult external auditors to avoid the situation in which employees become blinkered to their own work.

The maintenance of information security is also an important point for small and medium-sized organisations. Although the audits will be less extensive than in large organisations, they must not be omitted in any case. Within the context of the annual management assessment, the topmost management level must also check whether there are new legal stipulations that must be taken into consideration or whether other framework conditions have changed.

7.5 Continuous improvement of information security

Ultimately, the review of the security process is intended to improve the process. The results should therefore be used to assess the effectiveness and efficiency of the selected security strategy and, if necessary, to adapt it. The security strategy must also be reviewed in the case of changes to the security objectives or framework conditions.

8 Security concept

8.1 Creating a security concept

To fulfil the information security objectives and achieve the desired level of security, an understanding regarding how the fulfilment of tasks and business processes depends on the confidentiality, integrity, and availability of information must initially be developed. For this, it must also be considered which damage causes such as force majeure, organisational shortcomings, human error, or also cyber risks threaten the business processes. Afterwards the decision must be made on how to deal with these risks. The following partial stages are required in detail:

Selecting a method for risk analysis [DOC]

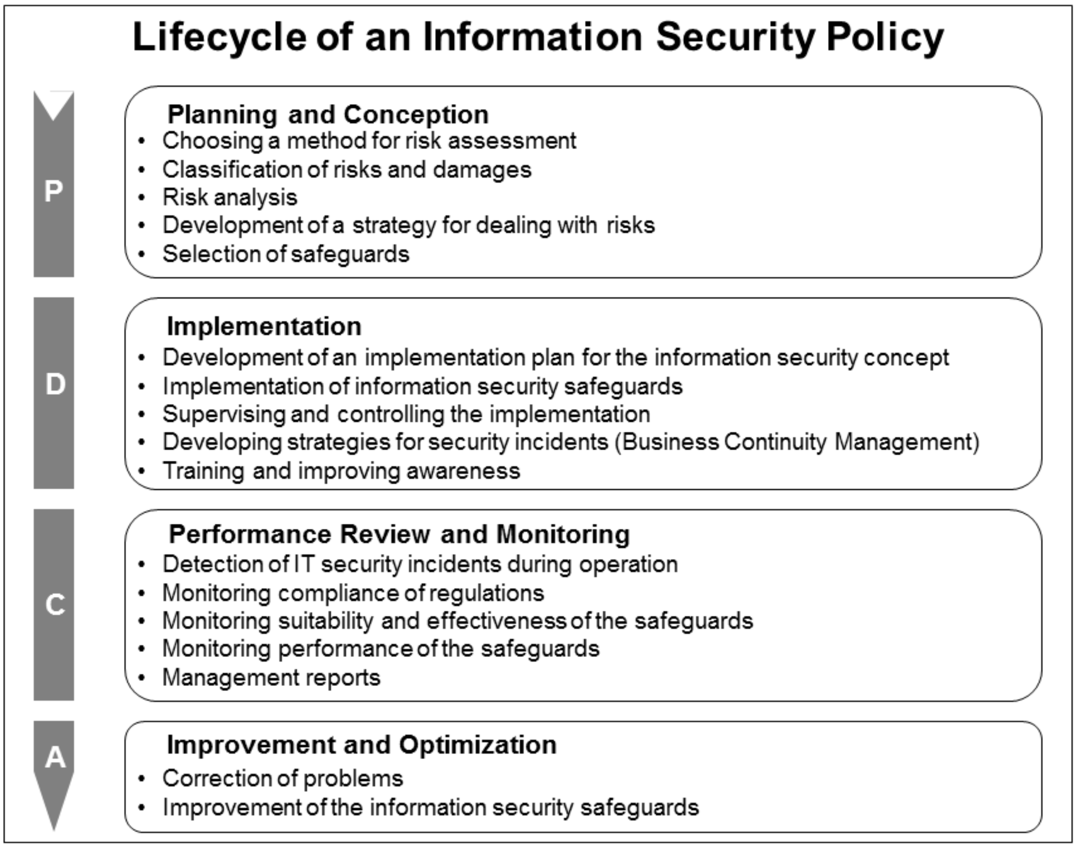
The risks that may be caused through damages for the business activity and tasks of an organisation by security incidents must be analysed. Thus, a method for risk analysis is an integral part of every information security management system. In order to be able to determine a risk, the basic threats must be determined, the damage potential and probability of occurrence must be assessed and compared to the risk acceptance of the organisation. Various risk analysis methods come into question depending on the use case, the organisational framework conditions, the type of industry, and the level of security that is aspired to. The information security management must select a method that is appropriate for the type and size of the organisation. The selected method has a decisive influence on the amount of work associated with the process of drawing up the security concept.

Various types of risk assessment are described in the ISO/IEC 31010 and ISO/IEC 27005 standards. The BSI developed a two-stage method derived thereof. When the methodology according to IT-Grundschutz is used, a risk assessment is performed implicitly for areas with normal protection requirements when drawing up the IT-Grundschutz modules. Only those threats which, after careful analysis, are shown to have such a high probability of occurrence or such drastic consequences that security safeguards must be implemented are considered in so doing. Typical threats that everyone must protect themselves against include, for example, damage due to fire, water, burglary, malware, or hardware defects. This approach has the advantage that IT-Grundschutz users do not have to carry out an individual basic threat and vulnerability analysis for a major part of the information system, since this analysis has already been performed in advance by the BSI. In certain cases, however, an explicit risk analysis must be carried out, for example if the information system considered includes target objects which

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

As a consequence, the above-described methodology will be complemented by the approach described in the BSI standard 200-3 *Risk analysis on the basis of IT-Grundschutz* (see [BSI3]), in the event of normal protection requirements.

The application of IT-Grundschutz bears the advantage that one’s own amount of work is reduced significantly, since IT-Grundschutz already describes a specific methodology and suggests suitable security requirements as well as security safeguards.



Lifecycle of an Information Security Policy

P

Planning and Conception
- Choosing a method for risk assessment
- Classification of risks and damages
- Risk analysis
- Development of a strategy for dealing with risks
- Selection of safeguards

D

Implementation
- Development of an implementation plan for the information security concept
- Implementation of information security safeguards
- Supervising and controlling the implementation
- Developing strategies for security incidents (Business Continuity Management)
- Training and improving awareness

C

Performance Review and Monitoring
- Detection of IT security incidents during operation
- Monitoring compliance of regulations
- Monitoring suitability and effectiveness of the safeguards
- Monitoring performance of the safeguards
- Management reports

A

Improvement and Optimization
- Correction of problems
- Improvement of the information security safeguards

Figure 6: Overview of the lifecycle of a security concept

Classifying risks and damages [DOC]

Depending on the selected method for risk analysis, the information security management must define how basic threats, potentials for causing damage, probabilities of occurrence, and the risks resulting thereof should be classified and assessed. However, it is difficult, complex, and moreover prone to error to determine individual values for damages and probabilities of occurrence. It is not advisable to invest too much time in the process of precisely determining probabilities of occurrence and possible damages. In most cases, it is more practical to work with qualitative categories both for the probability of occurrence and for the potential extent of damages. Per dimension, a maximum of five categories should be selected, e.g.

- Probability of occurrence: rarely, medium, frequently, very frequently
- Potential extent of damage: Negligible, Limited, Considerable, Threatening the existence of the organisation

Once these kinds of categories have been suitably defined in the organisation, they can be used as a basis for qualitative risk examination.

Risk analysis [DOC]

Every risk analysis must comprise the following steps:

- The information and business processes that are to be protected must be identified.
- All the relevant basic threats pertaining to the information and business processes to be protected must be identified.
- Vulnerabilities which the basic threats can use to take effect must be identified.

- The possible damages due to a loss of confidentiality, integrity, or availability must be identified and assessed.
- The assumable repercussions on the business activities or fulfilment of tasks through security incidents must be analysed.
- The risk of suffering damages due to security incidents must be assessed.

The terms “basic threat”, “vulnerability” and “risk” are defined in the glossary.

Developing a strategy for dealing with risks [DOC]

The topmost management level must specify how the identified risks should be dealt with. Depending on the risk appetite of an organisation, different risk acceptance criteria are possible in each case. Risk appetite refers to an organisation’s tendency regarding the assessment and dealing with risks, with this tendency resulting from cultural, internal, external, or economic influences. The risks identified must be processed accordingly by the information security management. The following options are available for this: risks can

- be avoided, for example, by excluding the cause of the risk,
- be reduced by modifying the framework conditions which contributed to the classification of risks,
- be transferred by sharing the risks with other parties, e.g. by outsourcing or through insurances,
- be accepted (based on a comprehensible state of facts), for example, because the opportunities related to the risk are to be seized.

The manner in which risks should be dealt with must be documented, assigned to a risk owner, and approved by the topmost management level. The resources necessary for implementing the strategy must be planned and made available.

When developing the strategy, the residual risk is an important decision criterion, in addition to the costs, that must be considered by the management level.

In practice, the risk assessment and risk handling steps are performed until the risk acceptance criteria of the organisation have been fulfilled and the remaining risk (“residual risk”) is thus in accordance with the organisation’s objectives and specifications. The residual risk must then be submitted to the management level for approval (“**risk acceptance**”). This documents in a traceable manner that the organisation is aware of the residual risk.

Within the framework of the risk assessment, mostly risks result exceeding the risk acceptance limit (see BSI standard 200-3) and therefore requiring handling. In the following, the risk handling option Reduction through the implementation of security safeguards is considered.

Selecting security safeguards [DOC]

Specific security safeguards can be derived from the general security objectives and security requirements specified by the management level. When selecting security safeguards, the cost-benefit aspects and practical feasibility must also be considered besides the effects on the level of security.

Besides technical security safeguards, organisational procedures and processes (such as user guidelines, the granting of rights, security training measures, as well as testing and approval procedures) must also be established. When doing so, the following issues, among other things, must be addressed:

- organisation (including specifying responsibilities, assigning duties and separating functions, regulating how information is handled, applications and IT components, hardware and software management, change management, etc.),
- personnel (e.g. briefing of new employees, making stand-in arrangements, etc.),

- training and awareness-raising for information security,
- identity and authorisation management,
- data backup (for all information, applications, and IT components),
- compliance and data privacy,
- protection against malware,
- protection of information during processing, transmission, and storage (e.g. through the use of cryptography),
- hardware and software development,
- detection of security incidents
- conduct during security incidents (incident handling),
- security audits (audits and revisions, penetration tests, etc.)
- contingency planning and maintenance of business activities in an emergency (business continuity),
- deleting and destroying of data, and
- outsourcing and cloud computing.

Comprehensible documentation must be provided explaining why the selected safeguards are appropriate for achieving the security objectives and requirements.

8.2 Implementation of the security concept

Once the security safeguards have been selected they must be implemented according to an implementation plan. The following steps should be followed during implementation:

Development of an implementation plan for the security concept [DOC]

An implementation plan must include the following subjects:

- specification of priorities (implementation sequence),
- specification of responsibilities for initiation,
- provision of resources by the management, and
- implementation planning of individual safeguards (definition of dates and costs, definition of persons in charge of implementation, as well as persons in charge of supervising the implementation and the efficiency of safeguards).

Implementation of the security safeguards

The planned security safeguards must be implemented in accordance with the implementation plan. In this, information security must be integrated in the pan-organisation procedures and processes. If difficulties arise during implementation, they should be communicated immediately so that solutions can be devised to overcome them. Typical solutions include, for example, modifying the lines of communication or the allocation of rights or adapting technical procedures.

Supervising and checking the implementation [DOC]

Regular checks must be performed to ensure that the set objectives are complied with. If objectives cannot be complied with, the member of the management level responsible for information security must be informed so that problems can be responded to in due time.

8.3 Performance review of the security concept

In order to maintain the level of security, the security safeguards identified as being appropriate must be applied on the one hand and, on the other hand, the security concept must be updated continuously. Furthermore, security incidents must be detected in due time and quick and appropriate reactions to these are required. The performance of the security concept must be reviewed at regular intervals. The effectiveness and efficiency of the implemented safeguards should be reviewed within the framework of internal audits. If the resources available are insufficient to have these kinds of audits performed by experienced internal employees, external experts should instead be charged with carrying out auditing activities.

Since the effort and expense for audits depend on the complexity and size of the information network, the audit requirements for small organisations are correspondingly lower than for large and complex organisations and can therefore normally be implemented very well. An annual technical check of the IT systems, a review of the existing documentation to check for its up-to-dateness, and a workshop intended to discuss problems and experiences with the security concept might already be sufficient in small organisations.

The following activities should be performed in detail:

Reaction to changes during routine operation

In the case of changes to routine operation (e.g. the introduction of new business processes, modifications to the organisation, or introduction of new IT systems), the security concept and its associated documents (such as a list of the spheres of responsibility or a list of the IT systems) must be updated.

Detection of security incidents during routine operation [DOC]

Safeguards must be implemented that allow information processing errors (which may compromise confidentiality, availability, or integrity), mistakes that are critical to security, and security incidents to be avoided as far as possible, to be limited in their impact, or at least noticed prematurely. The handling of errors must be documented. This includes that the implemented safeguards, the effects, and possibly resulting consequential safeguards are documented. In order to prematurely detect security issues, for example, system and network monitoring tools, integrity checks, logging of access activities, actions or errors, access controls to buildings and rooms, or fire sensors, water sensors, and air-conditioning sensors may be used.

The records and logs of the detection safeguards must be evaluated regularly.

Checking that the requirements are being complied with [DOC]

Regular checks must be performed to see whether all the security safeguards are being applied and implemented as planned in the security concept. This must involve checking that the technical security safeguards (e.g. regarding the configuration) and the organisational regulations (e.g. processes, procedures, and operations) are complied with. Checks should also be performed to ensure that the resources necessary for correct implementation of the safeguards are available and that everyone who has been assigned specific roles for implementing security safeguards is indeed fulfilling their obligations.

Checking the suitability and effectiveness of security safeguards [DOC]

Regular checks must be performed to determine whether the security safeguards are appropriate for achieving the security objectives that have been set. Their suitability can be assessed, for instance, by evaluating past security incidents, interviewing employees, or performing penetration tests. This also involves following the relevant developments in the environment of the business processes or the specialised tasks of the organisation. The technical or regulatory framework conditions, for instance, might have changed. To ensure their level of knowledge stays up to date, the persons responsible for security should, for example, use external sources of knowledge, visit symposia, and analyse standards and technical literature and information from the Internet. If the knowledge or time necessary in this regard is not available internally, external experts should be consulted.

In this context, it is useful to examine whether the security safeguards being used are efficient or whether the security objectives could be achieved with other safeguards that use resources more sparingly. In so doing, it must also be checked whether processes and organisational regulations are practicable and efficient. This frequently results in an opportunity for implementing necessary organisational improvements and restructuring measures.

Management assessments [DOC]

The management level must be kept informed about the results of the audits at regular intervals and in an adequate manner by the information security management. This includes pointing out problems, successes, and potential improvements.

The management reports must contain all the information regarding the management of the security process that is necessary for the management level. Such information includes, for example:

- overview of the current status in the security process,
- assessment of follow-up safeguards implemented after previous management assessments,
- feedback from customers and employees, and
- overview of newly occurred basic threats and security vulnerabilities.

The management level takes note of the management reports and makes the necessary decisions, for example, pertaining to improvements to the security process, the demand for resources, as well as the results of security analyses (e.g. reduction or acceptance of risks).

8.4 Continuous improvement of the security concept

Regularly reviewing the performance of the security concept serves for remedying errors and vulnerabilities identified and for optimising security safeguards with regard to their efficiency.

One important item involves improving the practical feasibility of technical safeguards and organisational procedures so as to increase the acceptance of the security safeguards. Likewise, the formulation of suitable security safeguards should time and again be considered as to whether it is easily comprehensible and understandable.

9 Certification of the ISMS

The successful design and operation of an ISMS are not an easy task. If this task has been performed successfully, it is practicable to document this both internally and externally and to render transparent the successful efforts in the field of information security. This may serve as a quality feature to both customers and business partners and therefore result in a competitive advantage as well. However, government agencies may also use this mechanism in order to improve the trust of the people in the security of their business processes and the related IT – particularly in the field if e-government. Another reason for aiming at a certification may result from compliance reasons, i.e. in order to demonstrate that relevant laws or contractual requirements are being met. Furthermore, this frequently results in a “passive” benefit, since other organisations may use an ISMS certificate in order to obtain information on the security status of potential partners.

ISO/IEC 27001 is a basic standard, on the basis of which an ISMS may be certified. It provides for a two-stage certification process: In this, the certificates are issued by independent certification bodies. The issuing of a certificate is preceded by an audit performed by a qualified auditor.

In order to ensure that the results of the certification audits are reproducible and repeatable, experienced and trained auditors are required. As a consequence, auditors must demonstrate that they have the necessary technical know-how and are familiar and comply with the specified scheme. All of the above is based on additional ISO standards in order to ensure the high quality and comprehensibility of certificates.

The standard and core safeguards of IT-Grundschutz map the requirements of ISO/IEC 27001. Therefore, it is also possible to have the successful implementation of IT-Grundschutz including the establishment of an ISMS certified by the BSI. The BSI developed a certification scheme for information security that takes into account the requirements regarding information security management systems from ISO/IEC 27001. The IT-Grundschutz compendium forms the audit catalogue for certification according to ISO/IEC 27001. As a consequence, it is referred to as ISO 27001 certification based on IT-Grundschutz. The IT-Grundschutz compendium as audit catalogue is provided at no charge by the BSI (as opposed to other certification bodies).

For an ISO 27001 certificate based on IT-Grundschutz to be issued, it is necessary to have an audit performed by an external auditor who is certified with the BSI. The result of the audit is an audit report that is presented to the certification body that will make the decision regarding the issuing of the ISO 27001 certificate based on IT-Grundschutz.

Additional information on the certification according to ISO/IEC 27001 can be found on the website of the BSI (see [ZERT]).

10 The ISMS based on BSI IT-Grundschutz

10.1 Introduction

The descriptions of an information security management system have been kept very generic in this document and in the ISO standards 27000, 27001, and 27002, and only serve as a framework. In practice, therefore, a great deal of freedom exists for the practical implementation of the generic specifications. The great challenge lies in establishing an ISMS in one's own organisation that not only helps to achieve the set security objectives, but is also cost-effective and economic.

In this, the question of how a security concept should be developed for the organisation is generally the most difficult one to answer. The main steps for developing a security concept involve assessing the risk and selecting the correct security safeguards. In so doing, selecting the method of risk analysis is particularly important, since the selected method has a decisive influence on the amount of work required to develop the security concept. The IT-Grundschutz methodology describes different approaches appropriate for the majority of use cases. Depending on the level of security aimed at and the information to be secured, it is possible to gradually get started regarding security management. When compared with the classical quantitative risk analysis, the IT-Grundschutz is much more cost-effective and has been tried and tested in practice for many years. As an added-value, the IT-Grundschutz methodology does not only describe how an ISMS works in principle, but, together with the IT Grundschutz compendium, it also portrays which specific security requirements should be complied with in practice. Practical explanations as to how the requirements of the modules of the IT-Grundschutz compendium may be complied with can be found in the corresponding implementation recommendations on the IT-Grundschutz.

As already mentioned above, the IT-Grundschutz methodology includes different approaches regarding the design of information security. The application of the basic safeguards approach offers first steps in the field of information security specifically for small and medium-sized organisations and helps designing a slender ISMS ("Bonsai ISMS"). As opposed to the standard safeguards, the fields of action of the basic safeguards do not form a closed cycle, but they are an initial approach that may be continued by using the standard safeguards.

This chapter provides an introduction to the essential elements of the IT-Grundschutz methodology and highlights that an approach in accordance with IT-Grundschutz is fully compatible with the ISO 27001 standard (see [27001]). A more detailed representation of the approaches according to IT-Grundschutz can be found in BSI standard 200-2 *IT-Grundschutz methodology* (see [BSI2]).

The IT-Grundschutz methodology describes an approach for establishing and maintaining an information security management system based on the IT-Grundschutz Methodology and the IT-Grundschutz compendium. The subjects mentioned here are explained therein in greater detail and in a more practice-related manner than in the present document.

10.2 The security process in accordance with IT-Grundschutz

All common methods, best practice examples, and information security management standards barely differ regarding the information they provide with regard to the security process or the duties of the management. The greatest differences lie in the manner in which the security concept is specifically developed, i.e. how the risk assessment is formulated and how the security safeguards are selected. Therefore, the basic approach for developing a security concept in accordance with IT-Grundschutz will be explained here.

10.2.1 Integrated risk assessment in IT-Grundschutz

A risk analysis in the field of information security differs in important areas from classical methods of actuarial mathematics or controlling. The precise calculation of the extents of damage and probabilities of occurrence normally performed in a “classical” or quantitative risk analysis frequently is not possible, since appropriate figures are not available. Even if a calculation is possible, interpreting the results remains very difficult.

Example: In the case of the classical risk analysis, the risk can be calculated by multiplying the extent of damage with the probability of occurrence. If, for instance, the destruction of a computer centre due to an aeroplane crash results in damages costing 20 million Euros and occurs statistically once every 20,000 years, the theoretical risk is 1,000 Euros per year. The same risk results if the damage caused through the theft of a notebook (without any loss of data) is estimated to be 2,000 Euros and occurs statistically once every two years. Although the value of the risk is the same in absolute terms, these two damage scenarios must be dealt with completely differently in the context of risk management.

Therefore, the IT-Grundschutz methodology already includes a risk assessment method providing the necessary information required to assess security incidents that are harmful to the business and, when compared to the quantitative method, that is easier to handle and sufficient for all cases under consideration. In IT-Grundschutz, it is assumed that, regardless of the type and orientation of an organisation, business-relevant information must be processed securely everywhere, commonly used and therefore comparable IT systems are being used, and comparable environmental conditions exist. As a consequence, there mostly are comparable basic threats. The security requirements of the business processes and specialised applications are specific to those processes and applications and may differ, in practice though, they usually lead to similar and comparable security requirements.

For the IT-Grundschutz methodology, the BSI, in the IT-Grundschutz compendium, analyses the basic threats and vulnerabilities for typical fields of application and components and uses this information to determine the resulting threats. In so doing, only those threats are considered which, after analysis, are shown to have such a high probability of occurrence or such drastic consequences that security safeguards must be implemented. Typical threats that everyone must protect themselves against include, for example, damage due to fire, burglary, malware, or hardware defects. This approach has the advantage that IT-Grundschutz users do not have to perform basic threat and vulnerability analyses or calculate probabilities of occurrence for a major part of the information network, since the BSI has already done this work for them.

Based on basic threats and the determined specific threats, the IT-Grundschutz compendium describes tried and tested technical, infrastructural, personnel, and organisational basic and standard requirements, as well as requirements in the case of high protection requirements for safeguarding typical objects.

A risk analysis must be performed for information and business processes that require a high or very high level of protection or for application environments that are not dealt with in the IT-Grundschutz. A simplified risk analysis according to the IT-Grundschutz methodology is described in BSI standard 200-3 *Risk analysis based on IT-Grundschutz* (see [BSI3]).

Both the risk assessment in accordance with IT-Grundschutz and the risk analysis described in [BSI3] are considerably more straightforward and more cost-effective than a quantitative risk analysis. The risk assessment in accordance with IT-Grundschutz furthermore has the advantage that organisations from the most different industries that use this method have a common and clearly defined basis for their risk assessment.

Classification of risks

The general requirement for classifying risks is accomplished in IT Grundschutz in the following steps:

1. Orientation on damage scenarios

Various damage scenarios should be examined in order to describe damages and the negative effects of security incidents as vividly as possible, for example:

- violations 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.

When simulating the scenarios, the damages that may arise due to a loss of confidentiality, integrity, or availability should be investigated.

For example, in the case of the "violation of laws" scenario, the discussion should, among other things, focus on the questions of which data must be handled in confidence and what the consequences would be if these conditions were breached due to negligence.

2. Classifying damages: definition of protection requirement categories

Performing a precise calculation of potential damages is mostly not reasonable or perhaps even impossible and is not necessary for selecting appropriate security safeguards either. It is therefore advisable to divide damages into a few classes. Attempting to calculate the damage "precisely" may even endanger security in many cases, since an inapplicable accuracy is suggested and those responsible are lulled into a "false sense of security" as a consequence.

Based on possible damages, three protection requirement categories are defined in the context of the IT-Grundschutz and are later used for classifying the items that are in need of protection (e.g. IT systems):

"normal protection requirements": the effects of the damage are limited and manageable.

"high protection requirements": the effects of the damage may be considerable.

"very high protection requirements": the effects of the damage may reach a catastrophic level that threatens the existence of the organisation.

Every organisation must define individually for every damage scenario how "normal", "high" and "very high" should be interpreted, i.e. which framework conditions should be applied for making the classification in the protection requirement categories. Since this has a direct effect on how risks are dealt with as well as on the demand for resources, this must be specified by the topmost management level of the organisation. The specification of protection requirement categories can vary greatly depending on the type and size of the organisation and only the topmost management level may define them specifically in cooperation with the security management. The BSI can therefore only provide examples for corresponding values that need to be adapted to suit the particular conditions.

Organisations may also use different protection requirement categories. In order to continue working with IT-Grundschutz in this case, it must be considered how the individual protection requirement categories can be mapped to those of the IT-Grundschutz. This may also lead to requirements from the IT-Grundschutz modules falling into different categories.

Example for the classification of financial damages:

> normal protection requirements exist when financial damages are considered tolerable for an organisation. For a small company, this may, for instance, mean that no damages exceeding 10,000 Euros must be allowed to occur due to security incidents. Higher protection requirements exist if damages would result in considerable financial losses, but would not threaten the mere existence of the company. In a small company, this may refer to a sum between

10,000 Euros and 100,000 Euros. Very high protection requirements exist when financial damages threaten the mere existence of the organisation. In a small company, this could be the case with a damage potential of over 100,000 Euros already. Other values would of course result for a large commercial bank.

10.2.2 Security concept

In addition to the standard safeguards, the IT-Grundschutz also offers two additional approaches for getting started with information security (basic and core safeguards). The IT-Grundschutz methodologies provide assistance in setting up and operating, as well as maintaining and improving the information security process in an organisation by revealing paths and methods for the general course of action, but also for solving special problems. The following steps must be performed in order to draw up a security concept according to IT-Grundschutz:

- Definition of the information network: specification of the scope

  At the beginning, the scope the security concept is to be drawn up and implemented for must be defined. For example, this may include certain organisational units of an organisation. However, this may also include areas processing defined business processes or specialised tasks, including the required infrastructure. In IT-Grundschutz, the scope for the security concept is also referred to as “information network”. The parts of the information network under consideration are the components to be protected using the appropriate modules of the IT-Grundschutz compendium.

- Structure analysis: identification of items to be protected

  Within the framework of the structure analysis, the relevant items to be protected, such as information, applications, IT systems, ICS systems, or IoT systems, networks, rooms, and buildings, but also responsible employees, must be determined for the information network under consideration, i.e. the scope or business process.

  During the structure analysis, the relationships and dependencies between the individual items to be protected must also be described. Documenting these dependencies mainly serves for identifying the effects of security incidents on the business activity so that an appropriate response can be provided.

  Example: if “server XY” is affected by a security incident, it is necessary to quickly find out which applications or business processes have been affected by this.

- Protection requirements determination: analysing the effects of security incidents on the business processes under consideration

  The degree of protection required is determined for each of the values determined during the structure analysis.

  Example: if the failure of an IT system may result in a great deal of damage, the determined value is high, since the IT system is characterised by correspondingly high protection requirements.

  The protection requirements of the business processes must first be determined. Building thereon, the protection requirements of the applications identified within the framework of the structure analysis can be determined. In so doing, it must be considered what type of information is being processed using these applications. In the vast majority of organisations, it is sufficient at this point to consider only very few information groups. Examples in this regard include customer data, publicly accessible information (e.g. address, opening hours), or strategic data for the management. Subsequently, it must be examined what information is processed where and using which IT systems.

  The protection requirements of the applications are transferred to the IT systems supporting the respective applications. The protection requirements of the rooms are derived from the protection requirements of the applications and IT systems operated therein.

Example: The business process involving the management of customer data is essential for maintaining business operations. This business process is executed on “server XY” consequently being characterised by high protection requirements. The room the server is located in therefore also has at least high protection requirements.

- Modelling: selection of the security requirements

  The modules of the IT-Grundschutz compendium describe specific threats and basic and standard requirements and requirements in the case of high protection requirements for typical tasks in information security management and fields of IT deployment. In this, organisational, personnel, infrastructural, and technical aspects of information security are considered in each case.

  The IT-Grundschutz compendium includes process modules from the following areas and layers:

  - ISMS: information security management,
  - ORP: organisation and personnel,
  - CON: concepts and approaches (e.g. crypto concept, software development),
  - OPS: operations (e.g. protection against malware, cloud computing), and
  - DER: detection and reaction (incident management, business continuity management).

  Furthermore, the IT-Grundschutz compendium includes system modules on

  - INF: infrastructure (e.g. buildings, computer centre),
  - SYS: IT systems (e.g. servers, clients),
  - NET: networks and communication (e.g. network architecture and design),
  - APP: applications (e.g. email and browser), and
  - IND: industrial IT (e.g. operational and control technology and control centre).

  Upon conclusion of the structure analysis, the business operations can be modelled with the help of these modules. In so doing, a collection of relevant IT-Grundschutz modules is assigned to the scope under consideration (information network). This results in a collection of security requirements that may serve as a basis for developing the security concept. The basic and standard requirements included in the IT-Grundschutz compendium and the requirements in the case of high protection requirements specify the generic requirements from ISO/IEC 27001 and ISO/IEC 27002. Furthermore, the implementation recommendations published for numerous IT-Grundschutz modules of the IT-Grundschutz compendium include specific implementation aids and numerous technical safeguards for the secure operation of typical IT, ICS, or IoT systems and applications. Precise instructions on selecting the modules (modelling according to IT-Grundschutz) help considering all the security-relevant aspects. This support also allows organisations to achieve their desired security objectives with considerably less or indeed no need for assistance from external consultants.

- IT-Grundschutz check: performing a target-performance-comparison

  The IT-Grundschutz check is an organisational instrument providing a quick overview of the present level of security. With the help of interviews, the status quo of an existing information network (modelled according to IT-Grundschutz) is determined in terms of the degree of implementation of the security requirements of the IT-Grundschutz compendium. The outcome of this check is a catalogue classifying the implementation status of each relevant requirement as “unnecessary”, “yes”, “partially”, or “no”. By identifying requirements that have not been met yet or have only been met partially, potential improvements regarding the security of the business processes under consideration and information technology are indicated.

- Risk analysis

Applying the IT-Grundschutz methodology allows for creating a level of security that is sufficient and appropriate for normal protection requirements. If the protection requirements for a particular area (such as an application or IT system) are higher or if no IT-Grundschutz modules exist for an area, a risk analysis should be performed after the IT-Grundschutz has been implemented.

The BSI has developed its own risk analysis method that is based on the implementation of IT-Grundschutz. It is described in BSI standard 200-3 *Risk analysis based on IT-Grundschutz* (see [BSI3]). However, a classical quantitative risk analysis may also be selected as the method for the areas concerned. If only a small area of information processing is affected, the effort required for an additional risk analysis is usually low. If, for example, only a specific IT system is affected which no IT-Grundschutz module exists for, consultation with the manufacturer or independent security consultant limited to this specific issue may generally already provide enough help to assess the risk and select appropriate security safeguards.

The combination of standard security safeguards and risk analysis for those areas whose protection requirements exceed the normal protection requirements is considerably more efficient than a complete quantitative risk analysis. Afterwards, the identified safeguards must be integrated and consolidated in the remaining security process.

- Implementation of the safeguards

  The identified security safeguards must be planned, implemented, supervised, and monitored. For this, the implementation sequence of the safeguards and who must implement which safeguards until when should be defined. All employees using and implementing security safeguards must be trained on the purpose of the safeguards and on what has to be considered during use.

11 Appendix

11.1 References

[20000] ISO/IEC 20000, IT Service-Management; among others consisting of ISO/IEC 20000-1:2011, Service management – Part 1: Service management system requirements and ISO/IEC 20000-2:2012, Part 2: Guidance on the application of service management systems, International Organization of Standardization (ISO)

[27000] ISO/IEC 27000:2016 “Information technology – Security techniques – Information Security management systems – Overview and vocabulary”, ISO/IEC JTC 1/SC 27

[27001] ISO/IEC 27001:2013 “Information technology – Security techniques – Information security management systems – Requirements”, ISO/IEC JTC 1/SC 27

[27002] ISO/IEC 27002:2013 “Information technology – Security techniques – Code of practice for information security controls”, ISO/IEC JTC 1/SC 27

[27005] ISO/IEC 27005:2011 “Information technology – Security techniques – Information security risk management”, ISO/IEC JTC 1/SC 27

[27006] ISO/IEC 27006:2015 ”Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems”, ISO/IEC JTC 1/SC 27

[27031] ISO/IEC 27031:2011 “Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity”, ISO/IEC JTC 1/SC 27

[31000] ISO/IEC 31000, International Organization for Standardization (Ed.), “Risk management – Principles and guidelines”, ISO/IEC, November 2009

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

[BSI3] Risk analysis based on IT-Grundschutz, BSI Standard 200-3, version 1.0, https://www.bsi.bund.de/grundschutz

[BSI4] Business continuity management, BSI Standard 100-4, version 1.0, https://www.bsi.bund.de/grundschutz

[BSIR] IS revision policy on the basis of IT-Grundschutz, BSI, https://www.bsi.bund.de/is-revision

[COBIT] COBIT (Control Objectives for Information and Related Technology), Version 5, ISACA, http://www.isaca.org/cobit

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

[ISF] The Standard of Good Practice 2016, ISF – Information Security Forum, 2016, https://www.securityforum.org/tool/the-isf-standardrmation-security/

[ITIL] IT Infrastructure Library (ITIL), IT-Service Management (ITSM), https://www.axelos.com/best-practice-solutions/itil, March 2017

[NIST80053] NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, NIST, 2015, http://csrc.nist.gov/publications/PubsSPs.html

[PCI] Payment Card Industry Data Security Standard (PCI DSS), version 3.2, PCI Security Standards Council (Eds.), April 2016, https://www.pcisecuritystandards.org

[ZERT] Information on the certification according to ISO 27001 on the basis of IT-Grundschutz, BSI, https://www.bsi.bund.de/iso27001-zertifikate