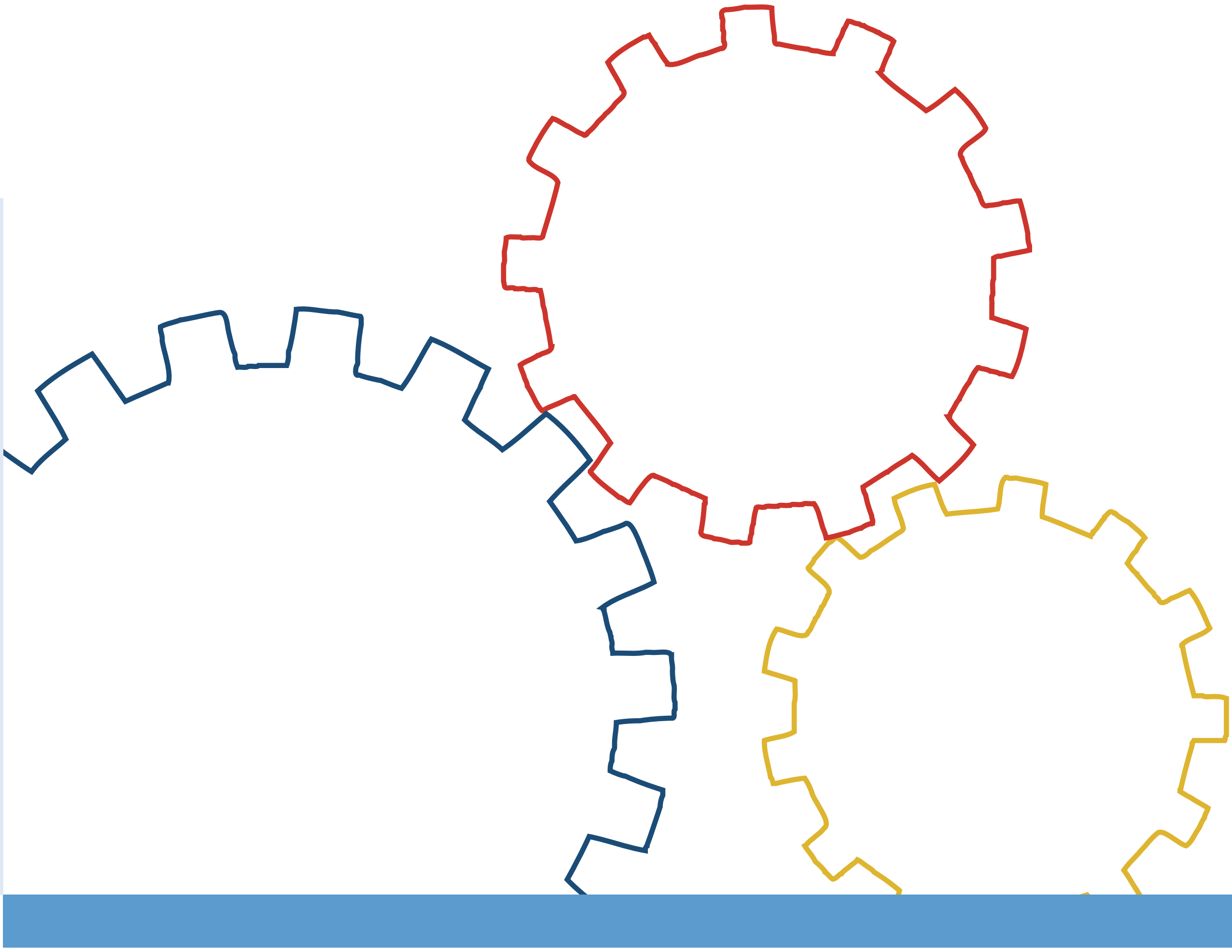
Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Standard 100-1

Information Security Management Systems (ISMS)



www.bsi.bund.de/grundschutz

Version 1.5

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

Contents

1. Introduction

1.1. Version history

As per	Version	Changes
December 2005	1.0	
Mai 2008	1.5	Stronger emphasis on the information security instead of the IT security, resulting in the modification of various terms Updated to reflect new and revised ISO standards

1.2. Aims

Information is an important value to companies and government agencies, and must therefore be protected appropriately. Most information today is created, stored, transported, or processed at least in part using information technology (IT). In the industry and administrations, no one denies the necessity to adequately protect its IT landscape. In addition, though, information from all other phases of business processes must be adequately protected. IT security incidents such as the disclosure or manipulation of information can have wide-ranging, adverse affects to a business or can prevent the organisation from performing its tasks, resulting in high costs.

No one in industry, commerce and administration would any longer dispute the need for adequate protection of their IT environment. IT security incidents can have far-reaching repercussions that harm business or interfere with the performance of tasks and thus result in high costs being incurred.

Practical experience has shown that optimising information security management frequently improves information security more effectively and lastingly than investing in security technology. However, measures originally implemented to improve information security can also have a positive effect outside a security context and can turn out to be profitable. Investments in information security can in many cases even contribute to cost savings in the medium term. Positive side-effects that can be expected from this are higher quality of work, increased customer confidence, optimisation of the IT landscape and organisational processes as well as the utilisation of synergy effects through better integration of information security management in existing structures.

An appropriate level of information security depends primarily on systematic procedures and only secondarily on the individual technical measures. The following considerations illustrate this hypothesis:

- The management level is responsible for ensuring statutory regulations and contracts with third parties are complied with and that important business processes are not disrupted.
- Information security has interfaces with many areas of an institution and affects highly important business processes and tasks. Only the administration/management level can therefore ensure that information security management is integrated smoothly in existing organisational structures and processes.
- Furthermore, the administration/management level is responsible for the efficient deployment of resources.

The administration/management level therefore has a high degree of responsibility for information security. A lack of supervision, an unsuitable information security strategy or wrong decisions can have far-reaching negative effects as a result of security incidents as well as missed opportunities and bad investments.

This standard therefore describes in a step-by-step fashion what it is that constitutes successful information security management and what tasks the administration/management level in public agencies and companies will be faced with in this context.

1.3. Target group

This document is aimed at persons responsible for IT operations and information security as well as IT security officers, experts, consultants and all interested parties entrusted with information security management.

Effective and efficient management of information security is not only an important issue for large institutions but also for small and medium-sized public agencies and companies as well as for the self-employed. The structure of an appropriate information security management system depends, of course, on the size of the institution. This standard and in particular the very specific recommendations of IT-Grundschutz are there to help any person responsible who wishes to improve information security within their sphere of influence. Throughout the following, we shall continuously provide information on how the recommendations of this standard can be adapted to suit the specific needs at hand whilst taking into account the size of the institution.

1.4. Application

This standard describes how an information security management system (ISMS) can be designed. A management system encompasses all the provisions as regards supervision and management so that the institution can achieve its objectives. An information security management system therefore specifies the instruments and methods that the administration/management level of an institution 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 with information security management?
- How can the IT security process be managed and monitored by the management responsible for this?
- How are security objectives and an appropriate IT security strategy developed?
- How are IT security measures selected and an IT security policy drawn up?
- How can an achieved level of security be maintained and improved?

This management standard provides a brief and 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 a step-by-step guide to developing an information security management system in practice and gives very specific measures for all aspects of information security. The procedure in accordance with IT-Grundschutz is described in the BSI standard 100-2 (see [BSI2]) and is designed such that an appropriate level of IT security can be achieved as cost effectively as possible. In addition to this, standard security measures for the practical implementation of the appropriate level of IT security are recommended in the IT-Grundschutz catalogues.

1.5. References

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

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

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

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

[ITIL] IT Infrastructure Library, Service Management - ITIL (IT Infrastructure Library) http://www.ogc.gov.uk/guidance_itil.asp, Januar 2008

[SHB] IT Security Manual – Manual for the Safe Application of Information Technology, BSI, Version 1.0 – March 1992, Bundesdruckerei

[OECD] Organisation for Economic Co-operation and Development (OECD), Guidelines for the Security of Information Systems and Networks, 2002, www.oecd.org/sti/security-privacy

[ZERT] Certification according to ISO 27001 on the basis of IT-Grundschutz - audit scheme for ISO 27001 audits, BSI, Version 1.2, March 2008, www.bsi.bund.de/gshb/zert

[ZERT2] Certification scheme for audit team leaders for ISO 27001 audits on the basis of IT-Grundschutz, BSI, March 2008, www.bsi.bund.de/gshb/zert

[13335] ISO/IEC 13335 "Management of Information and Communications Technology Security", ISO/IEC JTC1/SC27

[17799] ISO/IEC 17799:2005 "Information Technology - Code of Practice for Information Security Management", ISO/IEC JTC1/SC27

[27001] ISO/IEC 27001:2005 "Information Technology - Security Techniques - Information Security Management Systems Requirements Specification", ISO/IEC JTC1/SC27

[27002] ISO/IEC 27002:2005 "Information technology - Security techniques - Code of practice for information security management", ISO/IEC JTC1/SC27

[27005] ISO/IEC 27005 (2nd FCD, 2008) "Information technology - Security techniques - Information security risk management", ISO/IEC JTC1/SC27

[27006] ISO/IEC 27006:2007 "Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems", ISO/IEC JTC1/SC27

2. Introduction to information security

What is information security?

The purpose of information security is to protect information of all kinds and from all sources. This information might be printed on paper, kept on computer systems or stored in the minds of the users. IT security primarily deals with protecting information stored electronically and with its processing.

The classic core principles of information security, namely confidentiality, integrity and availability, form the basis for its protection. Many users also include additional basic values in their examinations. They can also be very helpful, depending on the corresponding application case. Additional generic terms used in information security include, for example, authenticity, validity, reliability, and non-deniability.

As the following examples illustrate, information security is not only threatened by wilful acts such as computer viruses, interception of communications or computer theft:

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

A choice of words: IT security versus information security

The terms "information technology", "information and communications technology" and "information and telecommunications technology" are frequently used synonymously. Due to the length of these terms, various abbreviations have become established and people therefore generally simply refer to IT. Since the electronic processing of information is a part of almost 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. Since, however, the term "IT security" is still predominantly used in the literature (among other reasons, because it is shorter), it will continue to be used in this publication as well as other publications of IT-Grundschutz, although the documents will place more and more emphasis over time on examining information security.

2.1. Overview of information security standards

In the area of information security, various standards have been developed in which emphasis is placed in part on other target groups or subject areas. The use of security standards in companies or government agencies not only improves the level of security, their use also makes it easier for organisations to agree on which security safeguards must be implemented in what form. The following overview points out the basic ideas behind the most important standards.

ISO standards for information security

In the international standards organisations ISO and IEC, it was decided to consolidate the standards for information security in the 2700x series since the number of standards is constantly increasing. The most important standards in this case are:

- ISO 13335

The ISO 13335 standard "Management of Information and Communications Technology Security" (formerly "Guidelines on the Management of IT Security") is a general guide for initiating and implementing the IT security management process. It provides instructions but no solutions for managing IT security. The standard is a fundamental work in this area and is the starting point or reference point for a whole series of documents on IT security management. The standard currently comprises the following parts:

- Part 1: Concepts and models for information and communications technology security management
- Part 2: Techniques for information security risk management
- Part 5: Management guidance on network security

The former parts 3 and 4 have been completely absorbed by the current parts 1 and 2. The ISO 13335-2 standard contains various methods for risk analysis. Certification is not intended.

- ISO 17799

  The aim of ISO 17799 "Information Technology – Code of Practice for Information Security Management" is to define a framework for IT security management. ISO 17799 is therefore primarily concerned with the steps necessary for developing a fully-functioning IT security management and for integrating this securely in the organisation. The necessary IT security measures are touched on briefly on the one hundred or so pages of the ISO/IEC 17799 standard. The recommendations relate to the management level and contain almost no specific technical information. Their implementation is one of the many options available for fulfilling the requirements of the ISO 27001 standard.

- ISO 27001

  Due to the complexity of information technology and the demand for certifications, numerous manuals, standards and national norms for information security have emerged over the past several years. The ISO 27001 "Information Technology – Security Techniques – Information Security Management Systems Requirements Specification" is the first international standard for management of information security that also allows certification. ISO 27001 provides general recommendations on around ten pages for, among other things, the introduction, operation, and improvement of a documented information security management system that also takes the risks into account.. The controls from ISO/IEC 27002 are referred to in a normative annex. The readers however, are not provided with any assistance for the practical implementation.

- ISO 27002

  The goal of ISO 27002 (previously ISO 17799:2005), "Information technology – Code of practice for information security management", is to define a framework for information security management. ISO 27002 is therefore mainly concerned with the steps necessary to establish a functioning security management system and anchor it in the organisation. The necessary security safeguards are only described briefly in the approximately 100 pages of the ISO standard ISO/IEC 27002. The recommendations are primarily intended for the management level and do not contain much specific technical information for this reason. The implementation of the security recommendations in ISO 27002 is one of many ways to fulfill the requirements of ISO Standard 27001.

  Note: Standard ISO 17799 was merged into ISO 27002 at the beginning of 2007 without making any changes to its contents in order to underscore the fact that it belongs to the ISO-2700x series of standards.

- ISO 27005

  This ISO Standard "Information security risk management" contains general recommendations for risk management for information security. Among other items, it supports the implementation of the requirements from ISO/IEC 27001. In this case, though, no specific method for risk management is prescribed. ISO/IEC 27005 replaces the previous standard ISO 13335-2. This standard, ISO 13335 "Management of information and communications technology security, Part 2: Techniques for information security risk management", provided guidelines for the management of information security.

- ISO 27006

  ISO Standard 27006 "Information technology - Security techniques - Requirements for the accreditation of bodies providing certification of information security management systems" specifies requirements for the accrediting of certification bodies for ISMS and also handles specific details of the ISMS certification process.

- Other standards in the ISO-2700x series

  The ISO 2700x series of standards will probably be made up of ISO standards 27000–27019 and 27030–27044 in the long term. all standards in this series handle different aspects of security management and are based on the requirements in ISO 27001. The other standards should contribute to improved understanding and the practical application of ISO 27001. They handle, for example, the practical implementation of ISO 27001, i.e. with the measurability of risks or with methods for risk management.

Selected BSI publications and standards for information security

IT-Grundschutz Catalogues

The BSI's best known publication on information security is the IT-Grundschutz Manual, which since first appearing in 1994 not only describes management of information security in great detail but also describes information security safeguards from the areas of technology, organisation, personnel and infrastructure in detail. Various areas of the IT-Grundschutz manual has not only been updated, but also have been restructured in 2005. This has resulted in the description of the methodology in accordance with IT-Grundschutz and the IT-Grundschutz Catalogues being separated from each other.

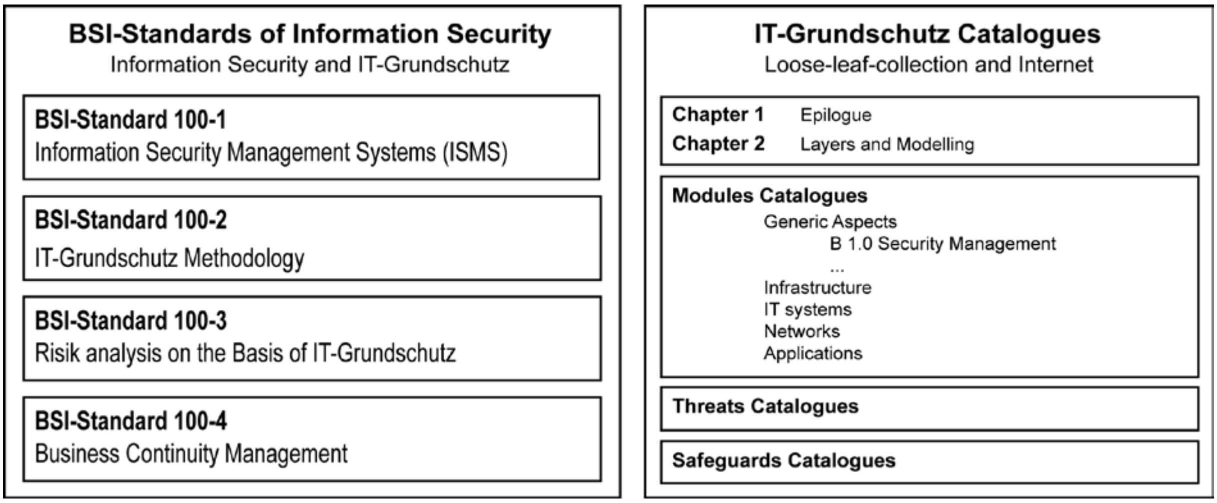

BSI-Standards of Information Security
Information Security and IT-Grundschutz
BSI-Standard 100-1
Information Security Management Systems (ISMS)
BSI-Standard 100-2
IT-Grundschutz Methodology
BSI-Standard 100-3
Risik analysis on the Basis of IT-Grundschutz
BSI-Standard 100-4
Business Continuity Management
IT-Grundschutz Catalogues
Loose-leaf-collection and Internet
Chapter 1 Epilogue
Chapter 2 Layers and Modelling
Modules Catalogues
Generic Aspects
B 1.0 Security Management
...
Infrastructure
IT systems
Networks
Applications
Threats Catalogues
Safeguards Catalogues

Figure 1: Overview of BSI publications on Information Security management

The IT-Grundschutz Catalogues have a modular structure and contain modules for typical processes, applications and IT components. In addition to recommending information security measures for each subject, they also describe the most important threats from which an institution should protect itself against. The user can therefore focus on the modules that are of relevance to their area. The modules of the IT-Grundschutz Catalogue are updated and extended regularly and also take into account the latest technical developments. They are therefore published as a loose-leaf corpus, on CD/DVD and also on the Internet. The IT-Grundschutz Methodology describes how information security solutions can be selected, developed and tested on the basis of standard security measures. This method has been published as BSI standard 100-2 from the BSI in the series of information security standards.

BSI series of standards for information security: the issue of IS Management

100-1 Information security management systems (ISMS)

The present standard defines the general requirements of an ISMS. It is fully compatible with the ISO 27001 standard and also takes the recommendations of the ISO 27001 and 27002 standards into consideration. It provides readers with an easy to understand and systematic instruction manual irrespective of which method they want to use to implement the requirements.

The BSI renders the content of these ISO standards in its own BSI standard so that it can describe some issues in greater detail and thus portray the content with a more didactical approach. Furthermore, the structure has been designed to be compatible with the IT-Grundschutz procedure. The standardised headers used in the documents mentioned above make it very easy for readers to get their bearings.

100-2 IT-Grundschutz Methodology

The IT-Grundschutz Methodology explains in a step-by-step fashion how an management system for information security can be developed and operated in practice. The functions of the information security management system and the organisational structure for information security are very important issues here. The IT-Grundschutz Methodology goes into great detail on how an policy for information security can be developed in practice, how appropriate information security safeguards can be selected and what should be watched out for when implementing the policy of information security. It also in detail answers the question of how to maintain and improve information security during routine operation.

IT-Grundschutz in conjunction with BSI Standard 100-2 therefore interprets the very general requirements of the previously mentioned ISO 27000, 27001, and 27002 standards and provides users with practical help in the form of numerous tips, background knowledge, information and examples. The IT-Grundschutz Catalogues not only explain what should be done but also provide very specific information on how this can be implemented (also on a technical level). Proceeding in accordance with IT Grundschutz is therefore a proven and efficient manner of fulfilling all the requirements of the above-mentioned ISO standards.

100-3 Risk analysis on the basis of IT-Grundschutz

The BSI has worked out a methodology for risk analysis on the basis of IT-Grundschutz. This approach can be used when companies or public agencies are already working successfully with IT-Grundschutz and would like to add an additional security analysis to the IT-Grundschutz analysis as seamlessly as possible.

100-4 Emergency management

BSI Standard 100-4 explains a method for establishing and maintaining an agency-wide or company-wide emergency management system. The method described here is based on the IT-Grundschutz Methodology described in BSI Standard 100-2 and complements them well.

ISO 27001 certification on the basis of IT-Grundschutz

The BSI certifies information domains, i.e. the interaction between infrastructural, organisational, personnel and technical components that enable business processes and tasks to be performed. The BSI certification involves auditing of the information security management system as well as auditing of the specific information security safeguards on the basis of IT-Grundschutz. The BSI certification always includes an official ISO certification in accordance with ISO 27001 but, due to the additionally audited technical aspects, is considerably more informative than pure ISO certification. The essential requirements for evaluating the information security management within the context of an audit result from the measures of the Grundschutz module entitled B 1.0 *Security Management*. The measures in this module are written such that the essential requirements of the BSI standard for information security management systems can be identified immediately. Figure 1 illustrates the standardised structure of the BSI documents. This standard describes audit criteria for auditors and certifiers.

To ensure conformity with ISO 27001, modifications were also made to the certification scheme for auditors and to the licensing scheme (see [ZERT]).

Other Standards

COBIT

COBIT (Control Objectives for Information and related Technology) describes a method for controlling the risks arising from the use of IT to support business-related processes. The COBIT documents are issued by the IT Governance Institute (ITGI) of the Information domains Audit and Control Association (ISACA). During the development of COBIT, the authors based their ideas on the existing standards for security management such as ISO 27002.

ITIL

The IT Infrastructure Library (ITIL) is a collection of several books on the subject of IT service management. They were developed by the United Kingdom's Office of Government Commerce (OGC). ITIL concerns the management of IT services from the point of view of the IT service provider. The IT service provider could be an internal IT department as well as an external service provider. The overall goal is to optimize and improve the quality and cost-effectiveness of IT services.

3. ISMS definition and process description

3.1. Components of an information security management system

Every company and public agency has a business management which in the following will be termed "management level" when referring to the actual managers themselves and when there is a risk of confusion with the term "management" as a leadership process (supervising, directing and planning).

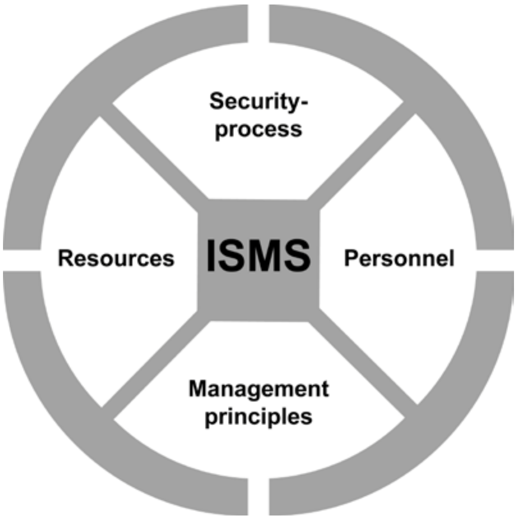


Figure 2: Components of an information security management system (ISMS)

A management system embraces all the policies pertaining to supervision and management for the purpose of achieving the institution'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 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
- Personnel
- Information security process
  - Policy for information security in which the information security objectives and strategies for their implementation are documented
  - Information security concept
  - Information security organisation

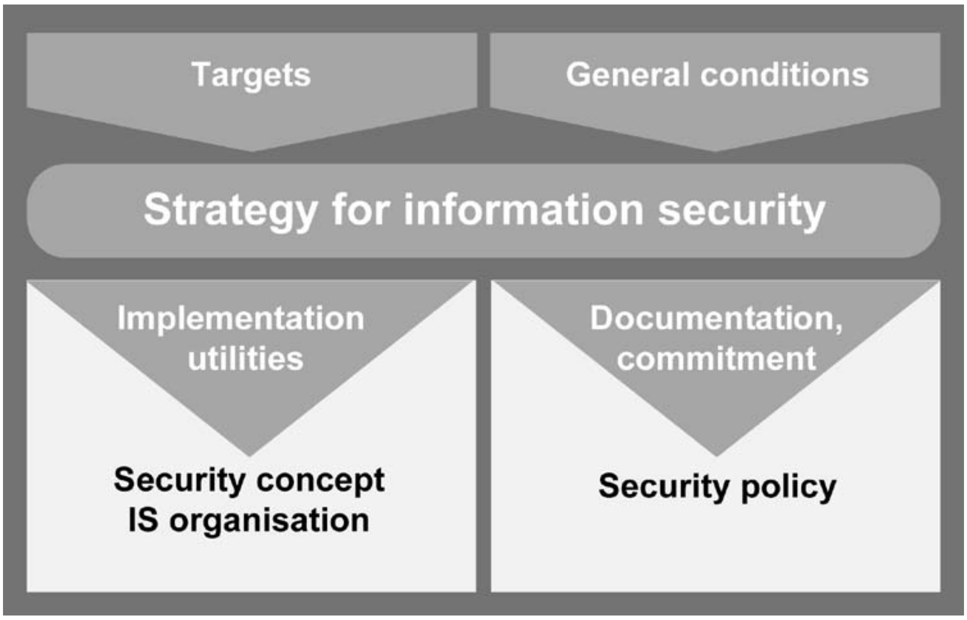


Figure 3: Strategy for information security as a central component of ISMS

Information security organisation and security policy are the tools that the management uses to implement its security strategy. Figure 3: *Strategy for information security as a central component of ISMS* and Figure 4: *Implementation of the information security strategy with the help of the policy for information security policy and an information security organisation* illustrate this interrelationship more clearly. The central points of the security strategy are documented in the *policy for information security*. The information security policy is of primary importance since it contains a visual record of the management level's commitment to its strategy.

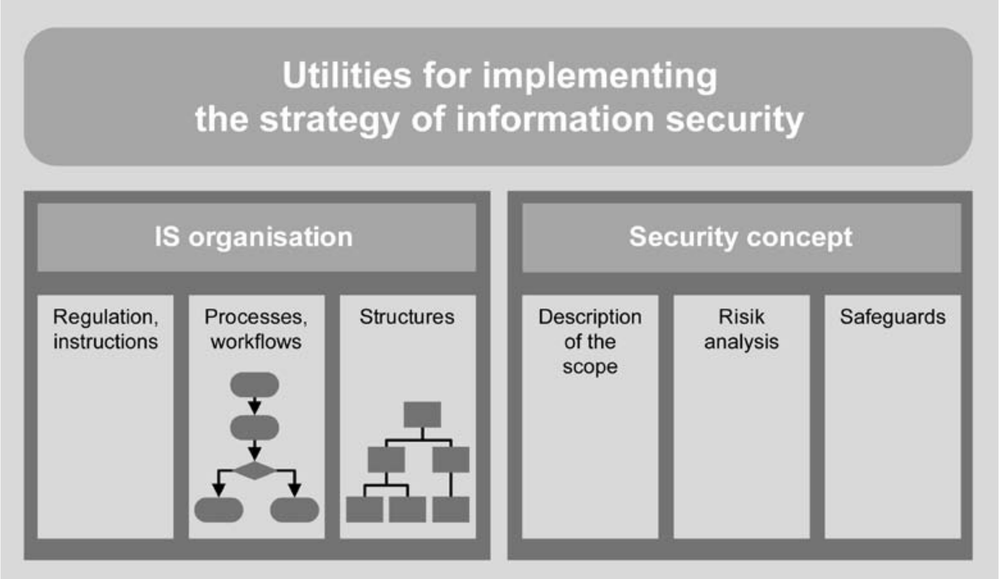


Figure 4: Implementation of the information security strategy with the help of the policy for information security and an information security organisation

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 and public agency is subject to continuous dynamic changes. Many of these changes also affect information security due to changes in the business processes, tasks, infrastructure, organisational structures and the IT. Besides the obvious changes within an institution, changes to the external conditions can also occur, for example, the statutory or contractual stipulations as well as the available information and communications technologies might change considerably. It is therefore necessary to manage security actively so that the security level that has been reached is also maintained over the long term.

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 information security measures. After information security measures 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 measures must be adapted and improved. These changes necessary due to the modifications must in turn also be replanned and implemented. If business processes are terminated or components and/or IT systems replaced or shut down, it will also be necessary to consider the associated information security issues, such as the withdrawal of authorisation or the secure erasure of hard drives. The information security safeguards are therefore subdivided into the following phases in the IT-Grundschutz Catalogues to ensure greater clarity for the reader:

1. Planning and design
2. Procurement (if necessary)
3. Implementation
4. Operation (measures for maintaining information security during normal operation including monitoring and performance review)
5. Disposal (if necessary)
6. Contingency planning

3.2.2. Description of the information security process

Not only business processes and IT systems have a "lifecycle". An policy for information security, information security organisation and ultimately the entire information security process all have a lifecycle. In order to describe the dynamics of the information security process as simply as possible, the information security process 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 monitoring the achievement of objectives
4. Eliminating discovered flaws and weaknesses and making optimisations as well as 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 model.

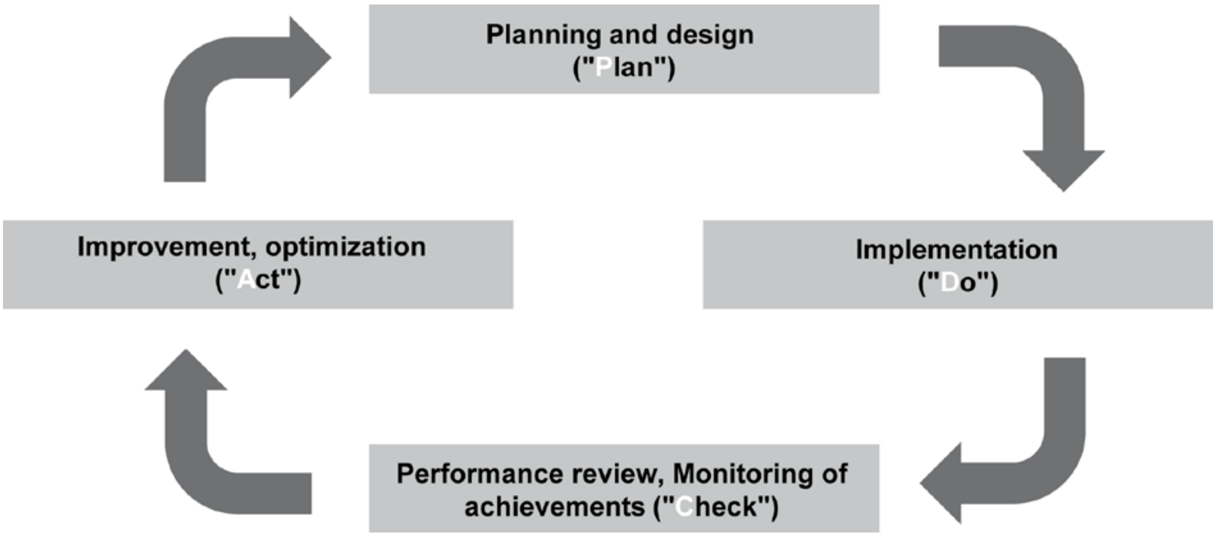


Figure 5: Lifecycle in the PDCA model according to Deming

The PDCA model is also included in the ISO 27001 standard. It can in principle be applied to all tasks within the information security process. The lifecycle of the policy of information security and the information security organisation can also be described very clearly using this model. The relevant chapters in this document therefore use the four phases of this model as their basis.

During the planning phase of the information security process, the prevailing conditions are analysed, the information security objectives determined and a security strategy developed containing the basic assumptions on how the set objectives should be achieved. The security strategy is implemented with the help of the security concept and an appropriate structure for the information security organisation. The security concept and the information security organisation must then in turn be planned and implemented and subjected to a performance review. The performance review carried out on the overlying information security process involves regularly examining whether the prevailing conditions (for example laws or corporate objectives) have changed and whether the security concept and information security organisation have proven to be effective and efficient.

However, since different institutions have different initial conditions, security requirements and financial resources, this procedure serves as a sound basis for orientation but must be adapted to their own needs by every public agency and company. Each institution must define and put into concrete terms the form of lifecycle model that is appropriate for them.

Small public 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 institution. In a very large company with many participating departments and individuals it is therefore probably necessary to have a more formal process that precisely defines what internal and external audits are needed, who should report to whom, who should draw up decision papers and when the heads 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 might be sufficient (at which they discuss the problems experienced throughout the past year, the resulting costs and the latest technological developments and other factors) in order to examine the success of the security process critically.

4. Management principles

Information security management, or IS management for short, is the term used for the planning and supervisory functions that are required to assure the meaningful development, practical feasibility and effectiveness of a well thought-out and systematic security process as well as all the information security safeguards required for this. This includes the fulfilment of legal requirements and following all relevant codes and regulations. There are various concepts dealing with the form that an efficient information security management system can take and which organisational structures would be expedient in such a system. Regardless of what form an IS management system takes, there are several basic principles that must be considered.

Some of the management principles presented here might sound somewhat trivial, since most managerial staff will consider them a matter of course. Paradoxically, however, it is precisely the simple things that are put into practice incorrectly or even omitted completely. Although discipline, patience, the ability to take on responsibility and prepare projects realistically and carefully are recognised values in many organisations in theory, they are not always put into practice. Particularly the less spectacular measures, such as process optimisation, training and motivation of staff or the drawing up of comprehensible documentation, are the ones that improve the level of security in practice quite substantially. Complex and therefore expensive measures, large-scale projects and investments in technology are frequently very wrongly portrayed as more effective and are often responsible for the poor reputation of security measures 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 points:

1. **Assumption of overall responsibility for information security**

   The topmost management level of every public agency and every company is responsible for the correct functioning of the institution in accordance with the institution's objectives 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 regulated in various laws. The management level as well as every individual manager must clearly demonstrate their commitment to their responsibility and must explain the importance of information security to all staff members.

2. **Integrating information security**

   Information security must be integrated in all the institution's processes and projects in which information is processed and IT utilised. This means, for example, that security requirements must not only be considered when procuring IT but also when designing business processes and training staff members.

3. **Managing and maintaining information security**

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

   - A strategy for information security as well as information security objectives must be agreed upon.
   - The impact of information security risks on the business operation and on the fulfilment of tasks must be investigated.
   - The organisational prevailing conditions for information security must be created.
   - Sufficient resources must be made available for IT operations and information security.

- The IT security strategy must be reviewed regularly and the achievement of objectives monitored. Any vulnerabilities and faults detected must be corrected. An "innovation-friendly" work atmosphere must be created for this and a will for continuous improvement demonstrated within the institution.
- Staff members must be motivated to take security issues seriously and to consider information security an important aspect of their duties. Adequate measures for training and making staff members aware of this must be provided, among other things.

4. Setting achievable goals

Projects frequently fail because the goals that have been set are unrealistic or too ambitious. This is no different in the area of information security. The security strategy must therefore be brought into accord with the resources that are available. In order to achieve a reasonable security objective, many small steps and a long-term continuous process of improvement without high investment costs can in the beginning be more efficient than a large-scale project. It can thus be appropriate to implement the necessary level of security initially only within selected areas. Then, however, using these areas as starting points, the security in the institution must be raised quickly to the aspired level.

5. Weighing up security costs against benefits

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

At this point it should be emphasised that information security is only ever achieved by interaction between technical and organisational measures. The investments in technology can be read in 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 carefully 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 staff members must be trained in how to use them. Technical solutions can also be replaced by organisational security measures. However, experience has shown that it is more difficult to ensure organisational measures are implemented consistently. Furthermore, doing so requires greater personnel input and thus also places a burden on resources.

6. The function of role model

The management level must assume the function of role model, also when it comes to information security. This requires, among other things, that the management level also complies with all the specified security regulations and takes part in training events.

4.2. Maintaining information security and making continuous improvements

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 continuously. This means that not only individual information security safeguards must be checked but also that the information security strategy must be reviewed on a regular basis.

The implementation of information security safeguards should be evaluated at regular intervals by means of internal audits. These also serve the purpose of collating and evaluating the experiences made in day-to-day practice. In addition to audits, it is also necessary to perform drills and implement measures for increasing staff awareness, since this is the only manner of determining whether all the specified procedures and staff conduct will actually have the desired effect in an emergency situation. Knowledge of vulnerabilities and opportunities for improvements must also, without exception lead to consequences within the information security organisation. It is also important that future developments in the technology used as well as in the business processes and organisational structures are perceived at an early stage so that potential threats can be identified in time, provisions made and security measures implemented. If significant changes in business processes or organisational structures appear on the horizon, the IT security management must also become involved. Even if its involvement is already planned for in the organisation's regulations, information security management should not wait to become involved as planned but should become integrated 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 institution, it might be useful to call in external auditors to avoid the situation in which staff members become blinkered to their own work.

The maintenance of information security is also an important point for small and medium-sized public agencies and companies. Although the audits will be of course, less extensive than in large institutions, they must not in any case be dispensed with. Within the context of the annual management appraisal, the topmost management level must also check whether there are new legal stipulations that need to be observed or if other prevailing conditions have changed.

Reviewing the information security process ultimately serves to improve it. The results should therefore be used to assess the effectiveness and efficiency of the selected security strategy and, if necessary, make changes to it. The security strategy must also be overhauled in the case of changes to the information security objectives or prevailing conditions. This issue is dealt with in detail in Chapter 7 of this standard.

4.3. Communication and knowledge

Communication is an important cornerstone for achieving the set information security objectives in all phases of the security process. Misunderstanding and a lack of knowledge are the most common reasons why security problems occur. A smooth flow of information regarding security incidents and security measures must therefore be assured on all levels and in all departments of an institution. This involves the following points:

- **Reports to the management level**

  The upper management must ensure it is kept informed regularly about problems, the results of reviews and audits, the latest developments, altered prevailing conditions and opportunities for improvement so that it can fulfil its management function.

- **Information flow**

  Inadequate communication and a lack of information can lead to IT security problems, wrong decisions and unnecessary working steps. This must be avoided with appropriate measures and organisational regulations. Staff members must be informed about the spirit and purpose of information security safeguards, particularly if these measures result in additional work or reduced convenience. Furthermore, any questions relating to information security or data protection from the employees arising in conjunction with their work should be answered. Moreover, users should be involved in the implementation planning of measures so that their own ideas are also considered and they are given the opportunity to assess the practical feasibility of these measures.

- **Documentation**

  To ensure the continuity and consistency of the entire information security process, it is essential that the information security process be documented. 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; processes therefore become measurable and repeatable. Documentation also aids in recognising fundamental weaknesses in the process and in avoiding repetition of errors. The documentation necessary for the various security activities fulfils different functions and is directed at different target groups. A distinction can be drawn between the following documentation types:

1. Technical documentation and documentation of work procedures (target group: experts)

   When malfunctions or information security incidents occur, it must be possible to restore the desired nominal conditions of the business processes and associated IT. Technical details and work procedures must therefore be documented such that this can be achieved within a reasonable amount of time.

   Examples of this are instructions for installing applications, backing up data, restoring data backups, configuring the PBX, 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 malfunctions and information security incidents occur.

2. Instructions for IT users (target group: IT users)

   Work procedures, organisational stipulations and technical information security safeguards must be documented such that information security incidents caused by a lack of knowledge or mistakes can be avoided. Examples of this are security guidelines for the usage of e-mail 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 users if they suspect an information security incident has occurred.

3. Reports for management tasks (target group: management level, information security management)

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

4. Recording management decisions (target group: management level)

   The management level must record and account for 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 of documentation:**

  Documentation does not necessarily have to be available in paper form. The documentation medium should be selected depending on requirement. For example, the use of a software tool might be helpful for emergency management. All the emergency measures and contacts should be entered into the tool in advance so that it can be used as a mobile application in an emergency situation. Furthermore, in the event of an emergency, this tool as well as all the required information and necessary IT systems must, of course, also be available for use, e.g. on a laptop. Depending on the type of emergency, it can however be more useful to have all the information ready at hand in paper form in a practical manual.

  Legal or contractual requirements as regards documentation may exist which must be observed, such as compulsory periods of record-keeping and required levels of detail. Documentation only actually serves a useful purpose if it is recorded regularly and kept up to date. It must also be labelled and filed such that it can be used when needed. The date and time each part of the documentation was created together with its author must be stated clearly. If references are made to other documents, the relevant sources must also be described. Additional reference documentation must likewise be available when needed.

Security-relevant documentation might contain information that needs protecting and must therefore be suitably protected. Besides the protection requirements, the storage type and duration as well as the available options for destroying information must also be specified. The process descriptions must describe whether and how the documentation must be evaluated.

- **Utilising available information sources and experiences**

  Information security is a complex issue, so the persons responsible for it must familiarise themselves with it very carefully. There are very many sources of information available that can be used for this. These include, among other things, existing norms and standards, Internet publications and other publications. Furthermore, co-operation with associations, peers, committees and other companies or public agencies as well as CERTs should be used for exchanging experiences about successful information security activities. Since the subject of information security is very broad, it is important to identify and naturally document the information sources and co-operation partners that are appropriate for the particular institution and the prevailing conditions.

5. Resources for IT operations and information security

Maintaining a particular level of information security always requires financial and personnel resources and time, which must be made available in sufficient quantities by the management level. If set objectives cannot be achieved due to lack of resources, it is not the fault of the persons responsible for implementation, rather, it is the fault of the superiors who have set unrealistic targets or have not made the necessary resources available. In order not to miss the set targets, it is important to conduct an initial cost-benefit comparison when the objectives are defined. In the course of the information 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, to guarantee the investments necessary for achieving an appropriate level of security.

Particularly since IT security is often associated only with technical solutions. This is another reason why it is better to use the term information security instead of the term IT security. However, it is especially important to point out that investments in personnel resources are frequently more effective than investments in security technology. Technology alone does not solve any problems; it must always be integrated in the prevailing organisational conditions. The examination of the effectiveness and appropriateness of information security safeguards must also be assured with the provision of sufficient resources.

In practice, the internal information security experts frequently do not have enough time to analyse all the influencing factors and prevailing conditions that are relevant to security (e.g. statutory requirements or technical questions). To some extent they are also not fully aware of the relevant underlying principles. It is always useful to fall back on external experts if questions and problems cannot be cleared up using one's own means. This must be documented by the internal information security experts so that the management level provides the necessary resources.

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

6. Involving personnel in the information security process

Information security concerns all personnel without exception. By acting responsibly and with quality awareness, every individual can avoid damages and contribute to success. Increasing the awareness for information security and providing appropriate training for staff members as well for as all management personnel are therefore fundamental prerequisites for information security. In order to be able to implement security measures as planned, personnel must have the necessary basic skills to do so. In addition to knowledge about how security mechanisms must be operated, this also involves an understanding for the spirit and purpose of security measures. The work atmosphere, common ideals and the commitment of personnel are all factors that decisively influence information security.

If newpersonnel are taken on 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 their job. If personnel leave the institution or their responsibilities change, this process must be accompanied by appropriate security safeguards (e.g. withdrawal of authorisation, returning keys and identity cards).

7. The information security process

The management level must be aware of all the relevant prevailing conditions and must specify information security objectives based on the company's business targets or on the public agency's mandate and must create the prerequisites required for their implementation. The procedure is planned with an security strategy to establish a continuous information security process. The security strategy is implemented with the help of an security concept and an information security organisation. In the following we shall therefore describe the relevant management activities for each lifecycle phase. Due to the broad range of activities and to maintain a clear overview, the activities relevant to the security concept will be described in a separate chapter.

7.1. Planning the information security process

Specifying the area of application within which the ISMS should apply [DOC]

An information security management system does not necessarily have to be introduced for an entire institution. The area of application within which the ISMS should apply must therefore be specified first. The area of application frequently includes the entire institution but it can also, for example, relate to one or more tasks, business processes or organisational units. In this case it is important that the considered tasks and business processes are completely contained within the selected area of application. Within the context of IT-Grundschutz, the term "information domain" is used for the area of application. It then also covers all the infrastructural, organisational, personnel and technical components that serve to fulfil the tasks in this area of application of information processing.

Ascertaining the prevailing conditions

The creation of information security is not an end in itself. Up-to-date and reliable information is the basis for most business processes. Information and communications technology should provide meaningful support for an institution's objectives and business processes. The following issues should at least be considered when developing the information security strategy:

- Objectives of the company or the functions of the public agency
- Legal requirements and regulations such as data protection, for example,
- Customer requirements and existing contracts
- Internal prevailing conditions (e.g. organisation-wide risk management or IT infrastructure)
- (IT-assisted) business processes and tasks
- Global threats to the business activities through information security risks (e.g. damage to the image, violation of laws, infringement of contractual obligations and theft of research results).

Formulating information security objectives and a policy for information security [DOC]

Information security objectives must be defined and strategic stipulations made on how the objectives should be achieved. The core statements are documented in an information security policy, also known as a policy for information security. The information security policy should at least contain statements on the following issues:

- Information security objectives of the public agency or company
- Relationship between the information security objectives and the business objectives or functions of the institution
- Aspired level of information security
- Guiding statements on how the aspired level of information security should be achieved
- Guiding statements whether and by what means the level of information security should be verified

- The policy is approved by the management and made public in the institution.

Establishing an information security organisation [DOC]

Planning an information security organisation involves specifying organisational structures (e.g. departments, groups, competency centers) as well as defining roles and duties. A manager from the topmost management level, such as a member of the management board, must be assigned responsibility for information security. Furthermore, at least one IT security officer must be nominated. The IT security officer must be able to file regular reports and independently of the topmost management level.

7.2. Implementing the policy for information security

A policy for information security must be drawn up in order to achieve the set information security objectives. For greater clarity, a separate chapter has been set aside to explain how a policy for information security can be planned and implemented and maintain the level of information security and improve it. The results of the check performed on the information security safeguards are then integrated in the performance review of the information security process and are assessed by the management level.

7.3. Performance review in the information security process

A performance review and evaluation of the information security process by the management level should be performed regularly (management appraisal). If and when the need arises (for instance, if information security incidents are occurring with increasing frequency or if there are serious changes to the prevailing conditions), meetings must also be held between the scheduled times. All results and decisions must be clearly documented [DOC].

The following questions, among other things, should be considered in the discussions:

- Have prevailing conditions changed that result in the need to change the procedure regarding IT security?
- Are the information security objectives still appropriate?
- Is the policy for information security still up to date?

The focus, when reviewing the performance of the information security process, is not on checking individual information security safeguards or organisational regulations but on viewing 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, entrust a service provider with the administration of the portal.

In this situation it is useful to examine how the security concept and the information security organisation have performed to date. In the chapter on security concept, various activities are described for reviewing the performance of individual information 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 information security safeguards are ineffective or decidedly expensive, this might be cause to reconsider and adapt the entire security strategy. The following questions should be asked:

- Is the security strategy still appropriate?
- Is the policy for information security appropriate for achieving the set objectives? Are, for instance, the legal requirements fulfilled?
- Is the information security organisation appropriate for achieving the objectives? Should its position in the institution be strengthened or should it be integrated more firmly in the internal processes?

- Is the effort (i.e. costs, personnel, materials) required to achieve the information security objectives in an appropriate relation to the benefit for the institution?

The results of the performance review must be consistently used to make appropriate corrections. This might mean that the information security objectives, security strategy or security concept need to be changed and the information security organisation adapted to the requirements. It might be useful to make fundamental changes to the IT landscape or to abandon or outsource business processes if, for instance, secure operation cannot be guaranteed using the available resources. If greater changes and more extensive improvements need to be made, this will result in a return to the planning phase thus completing the management cycle.

8. Security concept

8.1. Development of the security concept

To fulfil the information security objectives and achieve the aspired level of information security, an understanding must first be developed for how IT risks can threaten the fulfilment of tasks and business processes depends on the confidentiality, integrity, and availability of information. Therefore it has to be examined, which threat scenarios like force majeure, organisational shortcomings, human failure or IT risks threaten business processes. Afterwards the decision must be made on how to deal with these risks. The following partial stages are required:

Selecting a method for risk assessment [DOC]

Possible damage to the business activities and tasks of an institution due to information security incidents must be analysed and assessed. A method for risk assessment is therefore an integral part of every information security management system. In order to be able to identify a risk, the threats must be ascertained and their potential for causing damage and the probability that they will occur must be assessed. There are various risk assessment methods that come into question depending on the application, organisational boundary conditions, type of industry and level of information security that is aspired to. The information security management must select a method that is appropriate for the type and size of the institution. The selected method has a decisive influence on the amount of work that must be invested in developing the policy for information security.

Various types of risk assessment are described in the ISO/IEC 27005 standard. The BSI has likewise developed several methods that are derived from this and has tested them in practice. A very practical methods for risk assessment is described in the IT-Grundschutz procedure and can be implemented with the help of the IT-Grundschutz Catalogues. This approach is complemented by the BSI standard 100-3 entitled "Risk analysis based on IT-Grundschutz".

Applying IT-Grundschutz or other best-practise approaches has the advantage that the amount of work needed is reduced considerably because the authors already describe a specific method and suggest appropriate IT security measures.

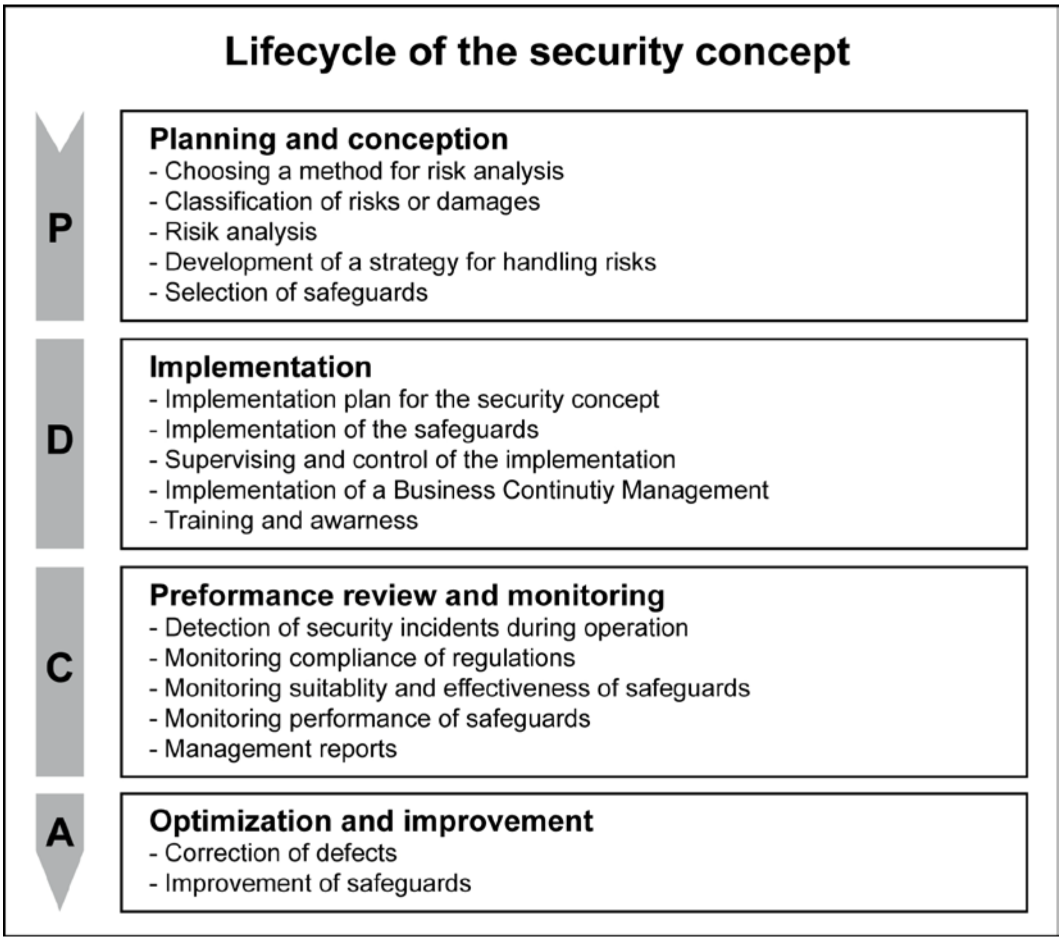

Lifecycle of the security concept
P
Planning and conception
- Choosing a method for risk analysis
- Classification of risks or damages
- Risik analysis
- Development of a strategy for handling risks
- Selection of safeguards
D
Implementation
- Implementation plan for the security concept
- Implementation of the safeguards
- Supervising and control of the implementation
- Implementation of a Business Continutiy Management
- Training and awarness
C
Preformance review and monitoring
- Detection of security incidents during operation
- Monitoring compliance of regulations
- Monitoring suitablity and effectiveness of safeguards
- Monitoring performance of safeguards
- Management reports
A
Optimization and improvement
- Correction of defects
- Improvement of safeguards

Figure 6: Overview of the lifecycle of an policy for information security

Classifying risks and damages [DOC]

Depending on the selected method for risk assessment, the information security management must ascertain how threats, the potential for causing damage, occurrence probabilities and the resulting risks should be classified and assessed.

However, ascertaining individual values for damages and occurrence probabilities is difficult, involved and moreover prone to error. It is not advisable to invest too much time in the involved (and error-prone) process of precisely ascertaining occurrence probabilities and possible damages. In most cases it is more practical to work with categories for both the occurrence probability and potential extent of damages. No more than 3 to 5 categories should be used, for example:

- Occurrence probability: rarely, frequently, very frequently
- Potential extent of damages: moderate, high, very high

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

Risk assessment [DOC]

Every risk assessment must comprise the following steps:

- The information and business processes that are to be protected must be identified
- All the relevant threats pertaining to the information and business processes that are to be protected must be identified
- Vulnerabilities which the 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 IT security incidents must be analysed
- The risk of suffering damages due to security incidents must be assessed

The terms "threat", "vulnerability" and "risk" are defined in the glossary in the IT-Grundschutz Catalogues.

Developing a strategy for dealing with risks [DOC]

The topmost management level must specify how the identified risks should be dealt with. The information security management must accordingly compile information about the risks. The following options are available for this:

- Risks can be reduced by implementing appropriate security measures
- Risks can be avoided, for instance, by restructuring or abandoning business processes or tasks
- Risks can be transferred, for instance, through outsourcing or insurances
- Risks can be accepted

The manner in which risks should be dealt with must be documented 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. The residual risk must therefore be assessed and likewise documented.

Selecting information security safeguards [DOC]

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

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

- 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 new staff members, making deputisation arrangements, etc)
- Training and increasing people's awareness on information security
- Data protection (for all information, applications and IT components)
- Computer virus protection
- Protection of information during processing, transmission and storage (e.g. through the use of cryptography)
- Hardware and software development
- Conduct during IT security incidents (incident handling)
- Contingency planning and maintenance of business activities in an emergency (business continuity)

- Outsourcing

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

8.2. Implementing the security concept

Once the security measures 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 issues:

- Specification of priorities (implementation sequence)
- Specification of responsibilities for initiation
- Provision of resources by the management
- Implementation planning for individual measures (specifying deadlines and costs and the specification of the persons responsible for the implementation and specification of deadlines as well as the persons responsible for checking the implementation and the effectiveness of measures).

Implementation of information security safeguards

The planned information security safeguards must be implemented in accordance with the implementation plan. In the process, information security must be integrated in the organisation-wide 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, for modifying the lines of communication or the allocation of rights as well as 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 time.

8.3. Performance review and improvement of the security concept

To maintain the level of information security, on one hand the information security safeguards that have been identified as being appropriate must be applied correctly and on the other hand the security concept updated continuously. Furthermore the information security incidents must be detected in time, and a rapid and appropriate response provided to deal with them. The performance of the security concept must be reviewed regularly. The effectiveness and efficiency of the implemented measures should be examined within the scope of internal audits. If not enough resources are available to have these kinds of audits performed by experienced internal members of staff, external experts should instead be charged with carrying out auditing activities.

Since the effort and expense for audits depends on the complexity and size of the information domain, the audit requirements for small public agencies and companies are correspondingly lower than for large and complex institutions and can therefore be implemented very well. An annual technical check of the IT systems, a review of the existing documentation to check how up to date it is, and a workshop at which the problems and experiences with the security concept can be discussed might already be sufficient in small institutions.

The following activities should be performed:

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 the associated documents (as well as a list of the spheres of responsibility or a list of the IT systems) must be updated.

Detection of information security incidents during routine operation [DOC]

Measures must be implemented that allow information processing errors (which can compromise confidentiality, availability or integrity), mistakes that are critical to security and information security incidents to be avoided as far as possible, to be limited in their impact or at least noticed early on. The following, for example, can be used to detect security problems at an early stage: tools for monitoring systems, integrity checks, keeping a log of access, actions or errors, controlling the access to buildings and rooms or fire sensors, water sensors and air-conditioning sensors.

The records and logs from the detection measures must be evaluated regularly.

Checking that the requirements are being complied with [DOC]

Regular checks must be performed to see whether all the IT security measures are being applied and implemented as planned in the security concept. This must involve checking that the technical security measures (e.g. as regards 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 measures are available and that everyone who has been assigned specific roles for implementing security measures is indeed fulfilling their obligations.

Checking the suitability and effectiveness of information security safeguards [DOC]

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

It is useful in this context to examine whether the information security measures being used are efficient or whether the information security objectives could be achieved with other measures that use resources more sparingly. The processes and organisational regulations should also be checked to see whether they are practicable and efficient. This frequently results in an opportunity for implementing necessary organisational improvements and restructuring.

Management appraisals

The management level must be kept informed about the results of the checks at regular intervals and in an adequate manner by the information security management. The problems, successes and opportunities for improvements should be pointed out.

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

- An overview of the current status in the information security process
- A report on the follow-up action taken after previous management appraisals
- Feedback from customers and staff members
- An overview of new threats and security vulnerabilities that have emerged

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

Regularly reviewing the performance of the information security process allows errors and vulnerabilities that have been detected to be remedied and the information security safeguards to be optimised as regards efficiency.

The activities here should not be limited to technical measures. It might also be necessary for staff members to receive training and have their awareness heightened. An important point also involves improving the practical feasibility of technical measures and organisational procedures so as to increase the acceptance of information security safeguards.

9. The BSI’s ISMS: IT-Grundschutz

9.1. 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 institution that not only helps to achieve the set security objectives but is also as cost-effective and economic as possible.

The question of how an security concept should be developed for the institution is generally the most difficult one to answer. The main procedures for developing an security concept involve assessing the risk and selecting the correct information security safeguards. Choosing the method of risk assessment is particularly important, since the method selection has a decisive effect on the amount of work required to develop an IT security policy. The procedure according to IT-Grundschutz describes a method that is appropriate for the majority of applications. Compared with classical quantitative risk analysis, it is much more cost-effective and has been tried and tested in practice for many years. As an added bonus, the IT-Grundschutz Methodology not only describes how an ISMS functions in principle but, together with the IT Grundschutz Catalogues, also portrays how specific measures might be implemented in practice.

This chapter provides an introduction to the essential elements of IT-Grundschutz Methodology and highlights that a procedure in accordance with IT-Grundschutz is fully compatible with the ISO 27001 ([27001]) standard. A detailed account of the IT Methodology in accordance with IT-Grundschutz is contained in the BSI standard 100-2 ([BSI2]).

The IT-Grundschutz Methodology describes an approach for establishing and maintaining an information security management system based on the IT-Grundschutz Methodology and IT-Grundschutz Catalogues. The issues mentioned here are explained there in greater detail and in a more practice-related manner than in the present document. Every module of the IT-Grundschutz Catalogues furthermore follows a lifecycle model and contains specific measures from the planning to the disposal phases.

9.2. The security process in accordance with IT-Grundschutz

All the most common methods, best practice examples and management of information security standards barely differ in the explanations that they provide regarding the security process or the duties of the management. The greatest differences lie in the manner in which the policy for information security is specifically developed, i.e. how the risk assessment is formulated and how the information security safeguards are selected. We shall therefore at hits point describe the basic procedure for developing a policy for information security in accordance with IT-Grundschutz.

9.2.1. Risk assessment

Risk assessment in information security

Risk assessment in information security differs in important areas from classical methods of actuarial mathematics or controlling. Precise calculation of the extent of damages and occurrence probabilities is usually not possible in a "classical" or quantitative risk analysis, since appropriate figures are not available. Even if a calculation is possible, interpreting the results remains very difficult.

Example: In the case of classical risk analyses, the risk can be calculated from multiplying the extent of damage with the occurrence probability. 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 in 20,000 years, the theoretical risk is 1,000 euros per year. This is the same as the risk of damages due to the theft of a notebook (without loss of data) estimated at 2,000 euros and occurring statistically once in two years. Although the value of the risk is the same computationally, these two damage scenarios must be dealt with completely differently in the context of risk management.

Furthermore, for many scenarios there are insufficient values based on experience available to allow reliable occurrence probabilities to be ascertained because, for instance, new technologies are being used or because there is not enough reliable basic information available. Even if sufficient data are available to allow the occurrence probability and extent of damage to be calculated fairly reliably for certain damage events, the development of a policy for information security on the basis of classical risk analysis is extremely involved and expensive. A well founded expertise and the processing of large amounts of data are required for an individual analysis of vulnerabilities for all essential business processes and the associated IT components as well as for the compilation of possible damage events including attribution of the occurrence probability and damage extent parameters.

The IT-Grundschutz Methodology therefore already includes a qualitative method for risk assessment that provides the necessary information for assessing information security incidents that are damaging to business. With the IT-Grundschutz Methodology, one assumes that the threats to secure operation of information processing are similar regardless of the type and orientation of an institution, business-related information needs to be processed securely everywhere in the organisation, common and therefore related IT systems used, and comparable environmental conditions exist. This means that comparable risks usually also exist although the security requirements of the business processes and applications are specific to those processes and applications and can differ, in practice though, they usually lead to similar and comparable security requirements.

For the IT-Grundschutz Methodology, the BSI analyses (in the IT-Grundschutz Catalogues) the vulnerabilities and threats for typical areas of application and IT components and uses this information to determine the resulting hazards. Only those threats which, after careful analysis, are shown to have such a high probability of occurring or such drastic consequences that information security safeguards must be taken are considered. Typical threats that everyone must protect themselves against include, for example, damage due to fire, burglary, computer viruses and hardware defects. This approach has the advantage that users of IT-Grundschutz do not need to perform threat and vulnerability analyses or calculate occurrence probabilities for a major part of the IT operations, since therefore a public agency has already done this work for them.

Based on the ascertained threats, the IT-Grundschutz Catalogues describe standard tried-and-tested technical, infrastructural, personnel and organisational security measures for typical objects.

Supplementary security analysis and possibly 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 IT risk analysis in accordance with the IT-Grundschutz Methodology is described in [BSI-3].

Both the risk assessment in accordance with IT-Grundschutz and the risk analysis described in [BSI-3] are considerably more straightforward and more cost-effective than a quantitative risk analysis. Risk assessment in accordance with IT-Grundschutz furthermore has the advantage that institutions from a wide variety of branches of industry 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 to damage scenarios

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

   - Violation of laws, regulations or contracts
   - Impairment of informational self-determination

- Physical injury
- Impaired performance of duties
- Negative internal or external effects
- Financial consequences

When running through the scenarios, the damages that can 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, centre around 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 in most cases not useful or perhaps even impossible, and is also not necessary for selecting appropriate IT security measures. It is therefore advisable to divide damages into a few classes. Attempting to calculate damage "precisely" can even endanger security in many cases, since this gives the false impression that a particular degree of precision has been achieved and those responsible are lulled into a "false sense of security".

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

"Normal protection requirements":	The impact of any loss or damage is limited and calculable.
"High protection requirements":	The impact of any loss or damage may be considerable.
"Very high protection requirements":	The impact of any loss or damage can attain catastrophic proportions which could threaten the very survival of the agency/company.

Every institution and for every damage scenario, one must specify how "normal", "high" and "very high" should be interpreted, i.e. which prevailing 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 institution. The specification of protection requirement categories can vary greatly depending on the type and size of the institution and only the topmost management level can specify them in cooperation with the information security management. The BSI can therefore only give examples for appropriate values which then need to be adapted to suit the particular conditions.

Examples for the classification of financial damages:

Normal protection requirements exist when financial damages are considered tolerable for an institution. In a small enterprise, this can mean that no damages exceeding 10,000 euros must be allowed to occur due to information security incidents. Higher protection requirements exist if damages would result in considerable financial losses but would not threaten the livelihood of the enterprise. In a small enterprise, this can lie between 10,000 euros and 100,000 euros. Very high protection requirements exist when financial damages threaten the livelihood of the institution. In a small enterprise, this could already be the case with a damage potential of over 100,000 euros. Other values would of course be arrived at for an institution like a large commercial bank.

Risk assessment

1. **Structure analysis:** identification of items to be protected [DOC]

   Within the framework of the structure analysis, the relevant items to be protected, such as information, IT applications, IT systems, networks, rooms and buildings as well as responsible staff members, must be ascertained for the examined information domain (i.e. area of application or business process).

   During the structure analysis, the relationships and dependencies between the individual items to be protected must also be described. By recording these dependencies in particular it is possible to identify the effects of information security incidents to business activities to be able to provide an appropriate response.

   Example: If "server XY" is affected by an information security incident, it is necessary to find out very quickly which applications or business processes have been affected by this.

2. **Assessing the protection requirements:** analysing the effects of information security incidents on the examined business processes

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

   Example: If the failure of an IT system can result in a great deal of damage, the value determined is high since the IT system has a correspondingly high protection requirements.

   In this case the protection requirements of the business processes must first be ascertained. On the basis of this, the protection requirements of the applications that were registered during the IT structure analysis can then be determined. In the process, one must consider what type of information is being processed with these applications. In most institutions it is sufficient at this point to consider only very few information groups. Examples of this are customer data, publicly accessible information (e.g. addresses, opening times) or strategic data for the management. Subsequently, one must examine what information needs to be processed where and with what IT systems in order to be able to accomplish the business processes.

   The protection requirements of the applications are also conferred upon the IT systems that support the particular applications. The protection requirements of the IT rooms are derived from the protection requirements of the applications and IT systems that are operated there.

   Example: The business process involving the management of customer data is essential for maintaining business operations. This business process runs on server XY which consequently has high protection requirements. The room in which the server is housed therefore also has at least a high protection requirement.

3. **Supplementary security analysis** [DOC]

   Application of the procedures in accordance with IT-Grundschutz enables a level of information security to be achieved 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 measures exist for an area, a supplementary security analysis should be performed after IT-Grundschutz has been implemented. The BSI has developed its own method for risk analysis for this purpose that is based on the implementation of IT-Grundschutz. It is described in the BSI standard 100-3 [BSI-3]. However, a classical quantitative risk analysis can also be chosen 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 for which no IT-Grundschutz module exists, consultation with the manufacturer or independent IT security consultant about this specific issue can generally already provide enough help to assess the risk and select appropriate information security safeguards.

The combination of standard security measures with supplementary 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 measures must then be integrated and consolidated in the remaining information security process.

9.2.2. Development of the security concept

The IT-Grundschutz Catalogues contain catalogues for typical modules, threats and measures. The modules contain descriptions of threats and standard information security safeguards for typical tasks of the information security management and areas of IT application. They consider the organisational, personnel, infrastructural and technical aspects of information security.

The IT-Grundschutz Catalogues contain modules from the following areas:

- Generic aspects of information security (e.g. organisation, personnel, contingency planning)
- Infrastructure security (e.g. buildings, computer centre)
- IT systems security (e.g. servers, clients, network components)
- Network security (e.g. network and system management)
- Security in applications (e.g. e-mail)

After the structure analysis, the business operations can therefore be modelled with the help of these modules. When doing so, a collection of relevant IT-Grundschutz modules is assigned to the area of application being examined (IT asset). This results in a collection of recommendations for IT safeguards that serve as a basis for developing the security concept.

The measures contained in the IT-Grundschutz catalogues comprise specific utilities to aid the implementation of the generic requirements in ISO 27001 or ISO 27002 as well as numerous technical measures for the secure operation of typical IT systems and applications. Precise instructions on selecting the modules help in ensuring all the security-relevant aspects (modelling according to IT-Grundschutz) are taken into consideration. This help also allows companies and public bodies to achieve their security objectives with considerably less or indeed no need for assistance from external consultants.