A publication of the ISACA Germany Chapter e.V.
Information Security Expert Group

Implementation Guideline ISO/IEC 27001:2013

A practical guideline for implementing an ISMS in accordance with the international standard ISO/IEC 27001:2013

ISACA®
Trust in, and value from, information systems
Germany Chapter

dpunkt.verlag

Publisher:
ISACA Germany Chapter e.V.
Oberwallstr. 24
10117 Berlin, Germany

www.isaca.de
info@isaca.de

Team of Authors:
- Gerhard Funk (CISA, CISM), independent consultant
- Julia Hermann (CISSP, CISM), Giesecke & Devrient GmbH
- Angelika Holl (CISA, CISM), Unicredit Bank AG
- Nikolay Jeliazkov (CISA, CISM), Union Investment
- Oliver Knörle (CISA, CISM)
- Boban Krsic (CISA, CISM, CISSP, CRISC), DENIC eG
- Nico Müller, BridgingIT GmbH
- Jan Oetting (CISA, CISSP), Consileon Business Consultancy GmbH
- Jan Rozek
- Andrea Rupprich (CISA, CISM), usd AG
- Dr. Tim Sattler (CISA, CISM, CRISC, CGEIT, CISSP), Jungheinrich AG
- Michael Schmid (CISM), Hubert Burda Media
- Holger Schrader (CISM, CRISC)

This guideline was translated from the German original version »Implementierungsleitfaden ISO/IEC 27001:2013« published in June 2016.

Last updated: April 2017 (final upon review by the Information Security Expert Group of the ISACA Germany Chapter)

Implementation Guideline ISO/IEC 27001:2013

A practical guideline for implementing an ISMS in accordance with the international standard ISO/IEC 27001:2013

ISACA®
Trust in, and value from, information systems
Germany Chapter

Foreword

An information security management system (ISMS) is a comprehensive set of policies and processes that an organization creates and maintains to manage risk to information assets. The ISMS helps to detect security control gaps and at best prevents security incidents or at least minimizes their impact. The implementation of an ISMS in accordance with the international standard ISO/IEC 27001 is, however, a very complex subject which includes many activities and resources and can take many months. Neverthless, for many organizations, an introduction is not only obligatory on the basis of contractual or legal requirements, but also a critical success factor in times of digital transformation and ever-increasing cybercrime.

The security of information and related technology is the concern of ISACA members worldwide. The goal of our members is to work to reduce the number of security incidents and to enable organizations to be better prepared for attacks and to react more effectively. To be successful in achieving this goal, the sharing of knowledge and experience is of primary importance. Therefore, on behalf of the Board of the ISACA Germany Chapter, we are pleased to present this work of our Information Security Expert Group to an international audience.

In 2014, the Information Security Expert Group decided to frame and develop a guideline for implementing an ISMS in accordance with ISO/IEC 27001:2013. This was first written and published in German. We believe that this guide, which has attracted a good response in German-speaking countries, will also be of great interest to an international audience. This is why we are especially grateful to the expert group for having supported a translation of their work with a lot of effort in adjustment, review, verification and quality assurance.

We would be glad if this outstanding work of the expert group facilitates the work of information security professionals worldwide and if it promotes knowledge sharing and exchange of experiences among them.

Matthias Goeken
Tim Sattler

Why do we need this guideline?

Information security is vital. However, as an aspect of corporate management, its aim must be to provide optimum support for business objectives. A well-structured information security management system (ISMS) designed in accordance with international standards provides an ideal foundation for efficient, effective implementation of a comprehensive security strategy, particularly in an era where cyber threats and cyber security are prevalent issues.

Whether the focus is placed on threats originating from the Internet, protecting intellectual property, complying with regulations and contractual requirements, or securing production systems depends on the situation at hand (e.g., industry, business model, attitude toward risk / risk appetite, etc.) and the respective organization's specific security objectives. Regardless of what the chosen approach is called, it is always important to identify and be aware of the information security threats that exist in the respective context and to select, implement, and consistently maintain the appropriate strategies, processes, and security measures.

The concrete implementation of an ISMS requires experience; however, first and foremost, implementation must be based on the decisions and obligations of the highest level of management in regards to this issue. The basic requirements for using an ISMS to support the business objectives include a clear mandate from management, a security strategy adapted to the business strategy, qualified personnel, and the necessary resources.

This *Implementation Guideline ISO/IEC 27001:2013* (in this document referred to as *Implementation Guideline*) includes practical recommendations and tips for organizations that already operate an ISMS in accordance with the international standard ISO/IEC 27001:2013, 'Information technology — Security techniques — Information security management systems — Requirements' or that want to set up this type of system, regardless of the certifications they hold or are attempting to acquire. The guide provides practical support and strategies for anyone responsible for setting up and/or operating an ISMS. It clearly outlines the benefits of an individually customized ISMS that also conforms to standards (if necessary). It also places particular emphasis on practical recommendations for establishing ISMS processes and/or improving existing ones, and it includes typical examples of how to implement various requirements.

Acknowledgment

ISACA Germany Chapter e.V. would like to thank the ISACA Information Security Expert Group and the authors who created this guideline: Gerhard Funk, Julia Hermann, Angelika Holl, Nikolay Jeliazkov, Oliver Knörle, Boban Krsic, Nico Müller, Jan Ötting, Jan Rozek, Andrea Rupprich, Dr. Tim Sattler, Michael Schmid, and Holger Schrader.

Project management: Oliver Knörle

Reviewers of the English version: Gerhard Funk, Julia Hermann, Oliver Knörle, Boban Krsic, Nico Müller, Dr. Tim Sattler. Special thanks to Elena Steinke who reviewed the document from both a professional and a native speaker perspective.

Contents

1. Introduction

The systematic management of information security in accordance with ISO/IEC 27001:2013 is intended to ensure effective protection for information and IT systems in terms of confidentiality, integrity, and availability.[1] This protection is not an end unto itself; rather, its aim is to support business processes, the achievement of business objectives, and the preservation of company assets by providing and processing information without disruptions. An ISMS generally employs the following three perspectives:

- **G – Governance perspective**
  - IT and information security objectives derived from overarching company objectives (e.g., supported by/ derived from COSO or COBIT)
- **R – Risk perspective**
  - Protection requirements and risk exposure of company assets and IT systems
  - Company's attitude towards risk
  - Opportunities vs. risks
- **C – Compliance perspective**
  - External regulations laid out by laws, regulators, and standards
  - Internal regulations and guidelines
  - Contractual obligations

These perspectives determine which protective measures are appropriate and effective for

- the organization's opportunities and business processes,
- the level of protection required in regards to the criticality of the company assets in question
- compliance with applicable laws and regulations.

Technical and organizational measures

Technical and organizational measures (TOMs) to achieve and maintain smooth and consistent information processing must be *effective* in order to achieve the required level of protection; they must also be *efficient*.

ISO/IEC 27001:2013, and the TOMs comprehensively and systematically laid out therein (various versions and quality levels of which are part of operating any ISMS), support the process of achieving the objectives initially laid out in terms of all three perspectives:

- the *governance perspective* refers to the control aspects of the ISMS, such as the close involvement of top management (see: Chapter *3.2 Leadership and Commitment*), consistent business and information security objectives (see: Chapter *3.3 IS Objectives)*, an effective and target group-oriented communication strategy (see: Chapter *3.9 Communication*), and appropriate policies and organizational structures (see: Chapter *3.5 Roles, Responsibilities and Competencies*).
- the *risk perspective*, which serves as a basis for transparent decision-making and prioritization of technical and organizational measures, is one of the key aspects of an ISMS in accordance with ISO/IEC 27001:2013. It is represented by IS risk management (see: Chapter *3.6 Risk Management*) and includes standards and methods for identifying, analyzing, and assessing risks in the context of information security – meaning risks that present a potential threat to the confidentiality, integrity, and/or availability of IT systems and information and, ultimately, the business processes that depend on them.
- the *compliance perspective* is firmly anchored throughout the entire standard. It comprises the definitions of the required (security) provisions, supported by the recommended controls in Annex A. Also addressed are the concrete implementation of these provisions, which must be ensured through regular monitoring by management and the Information Security Officer (see: Chapter *3.7 Performance Monitoring & KPIs*) and by internal audits (see: Chapter *3.12 Internal Audit* and *3.14 Continuous Improvement*). Appropriate documentation (see: Chapter *3.8 Documentation*) and a reasonable level of awareness of security issues among employees and managers (see: Chapter *3.10 Competence and Awareness*) are also vital from the compliance perspective.

1 Authenticity and non-repudiation can be viewed as secondary integrity objectives.

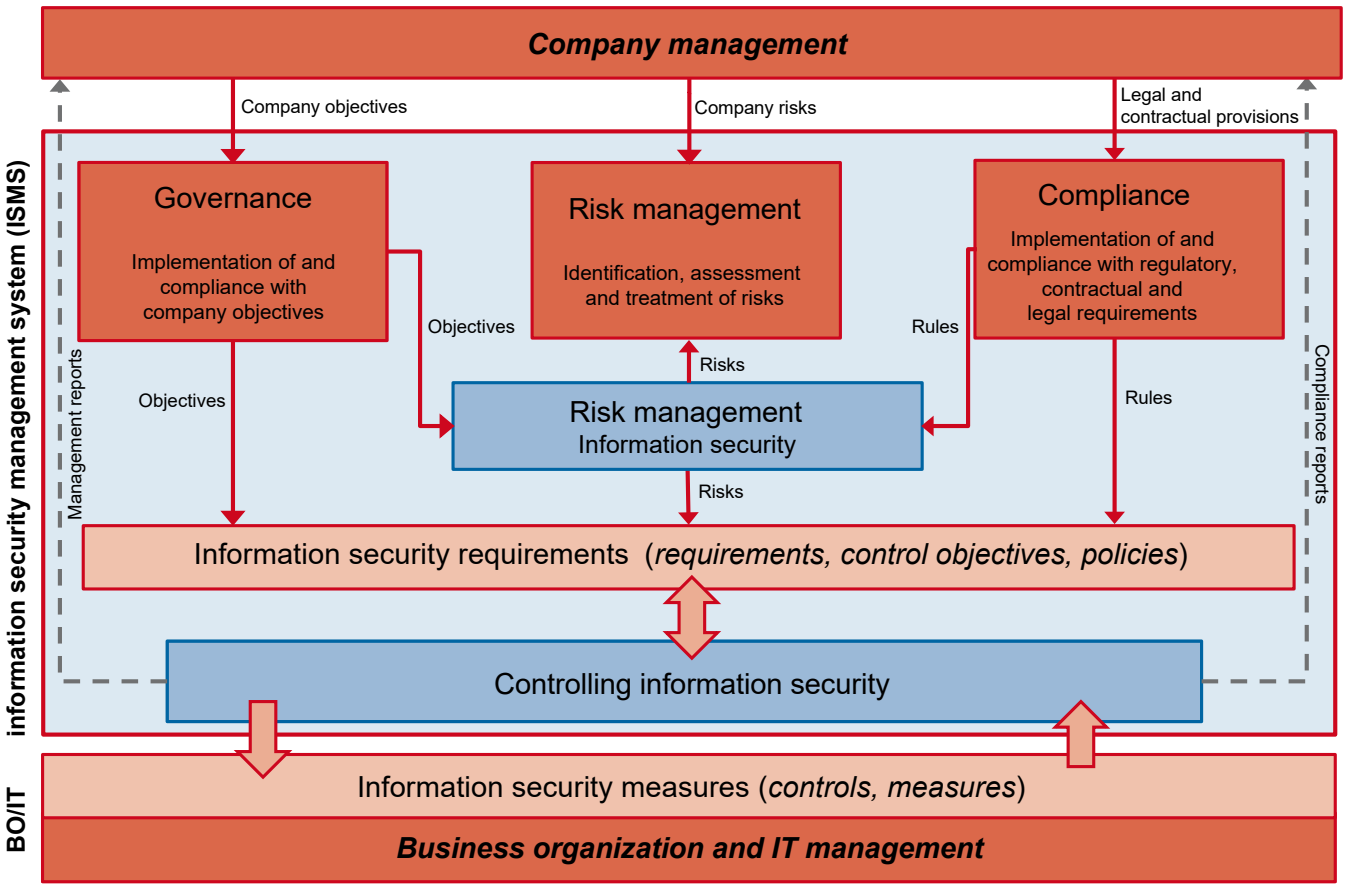


Figure 1: Incorporating the ISMS into corporate control processes[2]

2 Source: Carmao GmbH

2. Guideline Structure

2.1 Subject Areas

This implementation guideline is based on the fundamental subject areas of the ISO/IEC 27001:2013 standard; however, it does not identically copy the clause structure of the standard. Rather, the relevant subject areas of an ISMS in accordance with ISO/IEC 27001:2013 are described as 'core components' or 'building blocks' that have proven relevant and necessary in the field. Against this backdrop, content from the affected clauses of the standard has been restructured and summarized in individual key subjects. According to the authors, the standard can essentially be broken down into the 14 components explained in the following. These components, taken together, comprise an organization's ISMS:

1. Context of the Organization
2. Leadership and Commitment
3. IS Objectives
4. IS Policy
5. Roles, Responsibilities and Competencies
6. Risk Management
7. Performance Monitoring & KPIs
8. Documentation
9. Communication
10. Competence and Awareness
11. Supplier Relationships
12. Internal Audit
13. Incident Management
14. Continuous Improvement

The following chapters lay out the key success factors for all components in regards to standard-compliant, practically oriented implementation.

Additionally, this guideline is primarily intended to provide practical assistance; therefore the explanation of the components extends beyond the content that would normally be required by ISO/IEC 27001:2013 (or ISO/IEC 27002:2013).

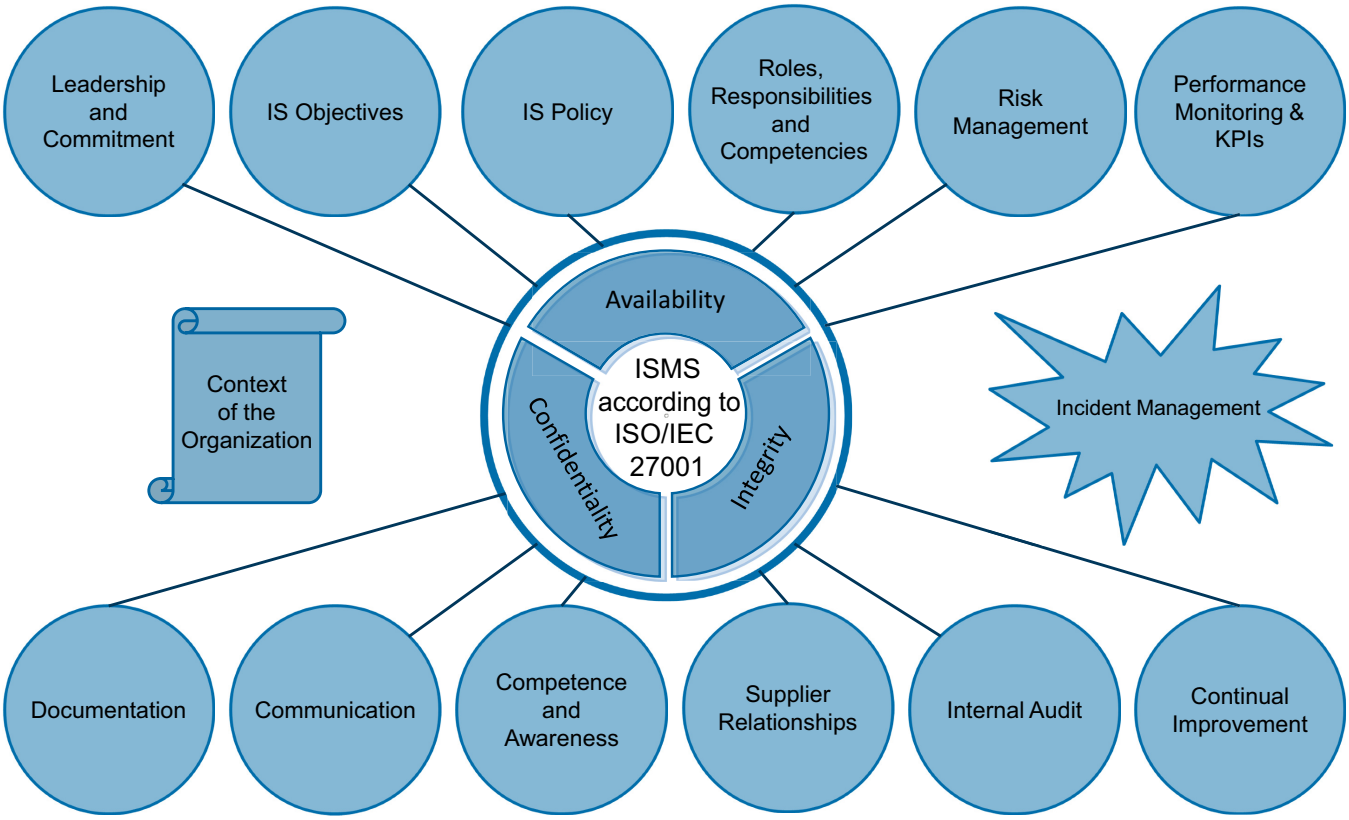


Figure 2: Components of an ISMS in accordance with ISO/IEC 27001:2013

Conversely, this also means that not all information provided in this document will be equally useful for all information security management systems or organizations.

Setting up an ISMS, regardless of whether it is done voluntarily or for a required certification, is an ambitious project that, like any other project, requires 'SMART'[1] objectives, sufficient professional resources, the right project manager, and a qualified team. Additionally, consistent, visible support from top management is vital for the successful completion of the project and the subsequent transition to ISMS operation.

In addition to providing assistance, the implementation guideline also includes references to other standards, frameworks, and other helpful sources (which are correspondingly labeled).

2.2 Chapter Structure

The individual chapters are all structured the same way and are broken down into the following three sections:

- **Success factors for practical implementation**
  This section lays out the success factors that the authors consider most important for setting up and operating an ISMS in accordance with ISO/IEC 27001:2013.
- **Documentation requirements**
  This section lays out the documentation requirements stipulated by the standard and recommended based on practical experience.
- **References**
  This section provides the clause numbers from ISO/IEC 27001:2013 that are relevant to the subject area, as well as any other sources that might be necessary or helpful.

2.3 Conventions

When the term '*standard*' is used throughout this document without further explanation, it always refers to the ISO/IEC 27001:2013 standard.

The term '*chapter*' refers to the various parts of this guideline; the term '*clause*' refers to the various parts of the standard.

The term '*appendix*' refers to the appendices to this guideline; the terms '*annex*' and '*Annex A*' refer to Annex A of the standard.

The terms '*organization*' and '*company*' each refer to the institution/department where the ISMS will be implemented. The terms are used interchangeably throughout the guideline.

1 SMART: specific, measurable, attainable, realistic, timely

3. Components of an ISMS in accordance with ISO/IEC 27001:2013

3.1 Context of the Organization

During the implementation of an ISMS, one of the first tasks is determining the accurate scope of the management system and the analysis of the requirements and the situation of the organization and its stakeholders.

Determining the scope

In accordance with the standard, the scope must be documented and, in addition to the processes and divisions covered by the ISMS, it should also include the results of the analysis of the requirements and situation.

- the scope document is primarily intended for the stakeholders of the management system, and if they request it, it should be provided to them. It is the only way that stakeholders (such as customers) can verify whether the ISMS covers the processes, infrastructure, subjects or requirements relevant to them.
- in practice, when organizations receive inquiries on this subject, they often refer to ISO/IEC-27001:2013 certificates that they hold, which, upon closer inspection, turn out to be irrelevant to or insufficient for the inquiry, because the process in question is not covered or only partially covered by the ISMS. To avoid any unpleasant and unintended surprises, the scope document and/or a *precise* description of the scope should be requested in addition to the certificate.
- another important document regarding the scope of an ISMS is the statement of applicability (SoA) required by the standard. The SoA includes explanations of the decisions to implement the controls in Annex A – i.e., whether the control in question is used within the ISMS or not, including an appropriate justification.
- a rough outline of the scope is usually provided in the information security policy. Unlike the scope document, the security policy and the SoA are generally categorized as internal documents and should not be passed on to external parties. However, as previously mentioned, close attention must be paid to the precise definition of the scope and the content of the SoA in the context of service provider relationships and, if applicable, service provider audits.

Situation Analysis

The purpose of the situation analysis is to place the ISMS into the overall environment based on its scope. In addition to the organizational and technical relations relevant to the ISMS, it should also include conditions that are typical for the respective industry or location. This must include the internal context, such as other management systems (ISO 9001:2015, ISO 22301:2012, etc.), as well as how it relates to other important departments such as risk management, human resources, data protection, audit and legal - if this is not already part of the existing scope. It must also include the external context, such as important suppliers and service providers, strategic partners, and any other relevant organizations.

Requirement Analysis

The persons in charge of the ISMS need to have a clear overview of the existing stakeholders, and their requirements for the organization and the management system.

The requirements of interested parties may include legal and official provisions (for example the German Federal Data Protection Act BDSG, the German Act against Unfair Competition UWG, the German Telemedia Act TMG, regulatory authorities, etc.) as well as contractual obligations. The organization itself (or an organization on a higher hierarchical level) might also have decision-making and/or policy-making authority, which must be taken into account.

Success factors for practical implementation

Determining the scope is the first and most decisive step in the process of setting up and operating an ISMS, therefore this phase should be carried out with extra diligence.

The context must be understood *before* any further actions (establishing and conducting risk analysis, organizational structure, defining and prioritizing tasks, project planning, etc.) are taken; this is also an important prerequisite for estimating the feasibility and the amount of work involved (resources, budget, time) in setting up and eventually operating the ISMS.

- lists are provided in ISO 31000:2009, Clause 5.3.2 '*Establishing the external context*' and Clause 5.3.3 '*Establishing the internal context;*' these lists help to ensure that the information provided is complete.

- the required level of detail for defining the scope is generally determined by internal and external information security requirements of the organization. In practice, it has proven helpful to describe the areas impacted by the ISMS in detail in the scope document, as this description is an important control instrument that is relevant for strategic decision-making and (future) coordination.
- the identification of stakeholders (and their requirements) as described in Clause 4.2 of the standard must be conducted carefully and comprehensively, as this is the only way to define clear objectives and content for the ISMS and to achieve the best possible benefit. Examples of stakeholders include: Owners, shareholders, supervisory board, regulatory authorities/lawmakers, customers, clients, suppliers, service providers, employees, etc.
- relevant external requirements can result from business plans, contracts, and regulations on the affected business processes set out by supervisory authorities and lawmakers, etc. In practice, support to determine these requirements is generally provided by someone in the (IT-) compliance role.

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- scope of the ISMS (Clause 4.3)
- statement of applicability (Clause 6.1.3 d)
- overview of all relevant legal, regulatory, and contractual requirements that have an impact on the information security strategy and the ISMS (A.18.1)

Additionally, the following documents have proven useful in practice:

- overview of all stakeholders relevant to the specific scope of the ISMS

References

ISO/IEC 27001:2013 – Clauses 4.3 and 6.1.3
ISO/IEC TR 27023:2015
ISO 22301:2012
ISO 31000:2009
ISO 9001:2015

3.2 Leadership and Commitment

A successful ISMS is implemented "top down" and establishes a connection between business objectives and information security by taking stakeholders' requirements into account, and by using effective measures to reduce risk to the operational business processes to an acceptable level.

To achieve this, the business objectives and requirements must be known, and the appropriate organization (such as the implementation/adaptation of risk management processes in the organization) must be put in place.

Approval and support from top management is indispensable to ensure a mandatory character and acceptance of the introduced management system processes.

The standard correctly and explicitly requires top management to take full and verifiable responsibility for information security within the organization. In addition, the importance of an effective ISMS and compliance with its requirements must be communicated to the affected employees. This is generally achieved by means of the information security policy (see Chapter 3.4 *IS Policy*).

- under the headline 'IT governance' and in relation to management's responsibility for strategy, particularly in areas subject to regulation, the supervisory authorities and boards are requesting verifiable proof of responsibility in an increasing manner.[1, 2]

Success factors for practical implementation

Definition, 'top management'

'Top management' refers to the level of management who is responsible for managing the organization that the ISMS is intended to protect and who makes decisions regarding the use of resources.

1 Joint Committee Report on Risks and Vulnerabilities in the EU Financial System, Chapter 7 (*http://www.esma.europa.eu/system/files/jc-2014-18_report_on_risks_and_vulnerabilities_in_the_eu_financial_system_march_2014.pdf*).

2 Erläuterung zu den MaRisk in der Fassung vom 14.12.2012, AT 4.2, AT 7.2 (*https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs1210_erlaeuterungen_ba.pdf?_blob=publicationFile&v=3) (German only*).

- according to the standard, 'top management'[3] at large corporations does not necessarily refer to the highest level of management in the entire organization (e.g., Board of Directors). It can also refer to the local managers or department managers responsible for the ISMS. The decisive factor here is the specific scope of the ISMS in question.
- during an external certification audit, a certification body may still require the involvement of the top management of the entire organization (for reasons of liability for risk). For this reason, it is advisable to address this issue with the certification body before launching the process of applying for the certification.

Tasks/responsibilities, 'top management'

ISO/IEC 27001:2013 requires members of top management to serve as role models on topics related to information security. In practical terms, this includes visible involvement in the process, obvious dedication to information security, as well as:

- compliance with information security requirements,
- making sufficient resources available in a transparent manner,
- requiring other levels of management to serve as role models,
- consistently dealing with and reacting to cases of nonconformity,
- self-commitment to continuous improvement.

The primary duties of top management in the context of ISMS are:

- taking full responsibility for information security
- defining the information security strategy and the concrete IS objectives (see Chapter *3.3 IS Objectives*)
- defining the decision-making criteria and principles for assessing and treating risks and implementing appropriate processes (see Chapter 3.6 *Risk Management*)
- integration of information security requirements into business processes and project management models (see Chapter *3.6 Risk Management*)
- conducting regular ISMS (top) management reviews (see Chapter *3.14 Continuous Improvement*)
- providing necessary financial and human resources to set up the ISMS and to implement the information security strategy

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- clause 9.3 '*Management Review*' requires documentation of the fact that top management monitors the ISMS, including the decisions regarding changes and improvements to the ISMS. They can be included in the risk treatment plan in the form of measures.
- results of a management review, such as decisions on options for continuous improvement, must be retained as documented information.

Additionally, the following documents have proven useful in practice:

- a document that records the derivation and assessment of risks resulting from existing discrepancies between the strategic IS objectives and the degree of objectives achieved, ideally in the form of a risk treatment plan.
- documents (presentations, logs, minutes, reports, etc.) which provide evidence for an effective reporting to the top management.

Note: There are several documentation options in the context of management responsibility. The examples above are suggestions for possible types of recording that contribute to making reporting and decision-making processes more transparent. Each organization must determine the type and frequency of documentation that works best.

References

ISO/IEC 27001:2013 – Clauses 5.1, 9.1 and 9.3

3.3 IS Objectives

The ISMS as a whole contributes to protecting and maintaining confidentiality, integrity, and availability of the respective business processes and the information contained therein. The company objectives laid out by company management and the IT objectives derived from the company objectives serve as the basis for designing/determining the information security objectives and the resulting controls.

Success factors for practical implementation

The objectives and principles of the ISMS are derived from the overarching company objectives, so failing to achieve IS objectives can have a direct impact on achieving company objectives. For this reason, it is vital to define appropriate and measurable IS objectives and ways to achieve them.

3 See Chapter *3.1 Context of the Organization* and ISO/IEC 27000:2014, Clause 2.84.

- the IS objectives must be aligned with the content of the IS policy.
- the IS objectives should always be based on the overarching company objectives, and they must be regularly reviewed to ensure they are up to date and still appropriate. This allows information security requirements to be integrated into operational business processes in such a way that it will not be perceived as additional work (or even an annoyance); information security becomes an integral component of day-to-day operations.
- the company's security requirements and the results of risk assessments are a further basis for selecting and defining IS objectives.
- when the IS objectives are being defined, it should be determined how these objectives will be achieved. This also involves identifying prerequisites for implementation. In addition to the primary tasks involved in achieving the objectives, the required resources and responsibilities as well as a timeframe and procedure for evaluating the implementation must be defined. In practice, this is often achieved by means of a direct reference to planned and ongoing projects. It is decisive that non-functional requirements – and security requirements are non-functional in most cases – are considered from the very beginning and integrated into the planning of projects, products, and systems (so called 'security-by-design').
- genuine, long-term objectives should be defined when drawing up IS objectives, rather than the operational technical/organizational measures required to achieve the objectives.
- like any type of objective, IS objectives should be 'SMART'[4] and aligned with all responsibles affected.
- the degree to which information security objectives are achieved must be measurable. Ideally, it is measured by KPIs that were defined in advance. Resources such as COBIT 5 for Information Security or The Definitive Guide to IT Service Metrics[5] can provide practical support for defining KPIs (see also: Chapter *3.7 Performance Monitoring & KPIs*).
- setting objectives that can be measured in a meaningful way, and carrying out those measurements can in practice be extremely challenging. It is therefore recommended to define a limited number of IS objectives as a first step toward implementing an ISMS. These objectives should be meaningful to the organization and should strike a balance between the effort required to implement them and the benefits they will deliver.
- the standard only requires IS objectives to be measurable 'if practicable.' In practice, 'if practicable' can be interpreted as slightly less strict than 'if possible.' This does not mean that measurements are not required by the standard; rather, the practicality of carrying out measurements must always be considered when the process is designed (see Clause 6.2 b).

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- documentation of the IS objectives must be made available.

Additionally, the following documents have proven useful in practice:

- the documentation of the IS objectives must be designed to include an implementation plan and/or references to specific processes. Generally, the IS policy already refers to the (documentation of the) IS objectives. The IS objectives can also be part of the IS strategy.

References

ISO/IEC 27001:2013 – Clause 6.2 COBIT 5 for Information Security
McWhirter, Kurt; Gaughan, Ted: The Definitive Guide to IT Service Metrics. IT Governance Publishing, 2012.

3.4 IS Policy

The (top) managers responsible for the organization are required to set out an information security policy (IS policy) that documents the organization's strategic decision to implement an ISMS, informs the target group about the obligation to comply with information security requirements as well as the self-commitment to continuously improve the ISMS.

The policy must suit the organization's purpose and include the principles and objectives that the ISMS seeks to achieve, as well as the organization's general information security objectives.

Success factors for practical implementation

The policy is an important tool for the organization; it supports the management in communicating the importance of an effective ISMS and of achieving compliance with ISMS requirements. Additionally, the policy incorporates the most important strategic and tactical objectives that the ISMS is intended to help achieve. Ideally, it will also include the ramifications and requirements that the affected staff members and divisions within the scope of the ISMS are facing.

4 SMART: specific, measurable, attainable, realistic, timely.
5 McWhirter, K.; Gaughan, T.: The Definitive Guide to IT Service Metrics. IT Governance Publishing, 2012.

Furthermore, the responsible managers must provide a complete yet brief description of the established ISMS, including its roles and responsibilities, in the policy. The following aspects must be considered:

- the IS policy must be adopted by the highest level of management (top management) and made available to the appropriate supervisory bodies.
- the IS policy must be available as documented information and be subject to transparent document control.
- the IS policy can include a reference to the company objectives and IT objectives.
- the language used in the IS policy must be in line with the company's conventions. It must appropriately highlight the significance of the document.
- employee training must ensure that all affected employees within the scope of the IS policy are familiar with the policy. The policy must be communicated to the affected employees and be made available to the stakeholders as required (see Chapter *3.10 Competence and Awareness*).
- to achieve the objectives, it is important for individual employees to be aware of their personal responsibility and their involvement in information security processes, as well as the specific requirements associated with relevant processes (which are derived from the IS policy and are reflected in subject-specific guidelines and work instructions).
- the IS policy should not be mixed with further documentation or implementation guidelines such as the content of security concepts or manuals. However, these sorts of 'downstream' documents can of course refer to the policy (or other relevant high-level ISMS documents) in order to make the 'order of guidelines' or 'chain of requirements' more consistent.
- depending on the ISMS approach chosen, the existing structure and the way work is organized within the company, it may make sense to design the IS policy as one complete, comprehensive information security document, or to make it an 'anchor' or 'starting point' for the subject that can be completed by further detailed documentation. In either case, it is important to ensure wording and scope are aligned to the objectives of the IS policy.
- although there are a range of templates and exemplary text blocks available for this purpose, it is recommendable to create the IS policy from scratch, i.e. as a new document that fully covers the organization's requirements. Templates can provide ideas and inspiration on how to structure the document and the type of content it should include. The key to a successful implementation of the policy and to achieving commitment of employees for information security is to ensure transparent alignment of the policy with existing company and IT objectives. Key messages should be recognizable among all documents.

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- information security policy (see Clause 5.2 e)

Additionally, the following documents have proven useful in practice:

- subject-specific information security policies and guidelines (see Annex A.5.1)
- associated documents and organizational charts, e.g., explaining the organizational structure in the context of information security (if not included in the policy)

References

ISO/IEC 27001:2013 – Clause 5.2

3.5 Roles, Responsibilities and Competencies

According to Clause 5.3 of the ISO/IEC 27001:2013 standard, the organization is required to define the roles required for an effective ISMS, as well as the responsibilities regarding the setup, maintenance, and continuous improvement of the ISMS. The resources required for the process must be determined and made available (see Clause 7.1).

In this context, management is required to assign responsibility and authority for the tasks relevant to information security and to communicate to the appropriate individuals accordingly. However, it must be ensured that roles are clearly structured and defined, and that potential conflicts of interest are avoided (e.g. by means of a RACI[6] or SoD[7] matrix).

6 RACI: Responsible, accountable, consulted, to be informed (see Glossary).
7 SoD: Segregation of duties (see Glossary).

Success factors for practical implementation

Specification of roles within the ISMS organization

At least the role of an information security officer (ISO) and/or a chief information security officer (CISO) should be established within the organization, although the requirements laid out in the standard refer to all responsibilities and authorizations relevant to information security (see Clause 7.2 a). Furthermore, the role "risk owner" and "asset owner" must be defined and established within the ISMS.[8]

Other roles in the context of information security – security administrators, internal auditors, etc. – must be defined and described.

- the description of the CISO/ISO role must also include the skills (experience, education, training, people skills, etc.) which are necessary for the job.
- the following conflicts of interest must be avoided:
  - Information security officer (ISO and/or CISO[9]) and Head of IT/CIO[10]
  - Data protection officer (DPO) and Head of IT/CIO
  - Internal ISMS auditor and IT administrator
- in certain cases, the roles of ISO/CISO and DPO can be held by the same employee. This combination is associated with a certain (unavoidable) conflict of interest though. The tasks of the DPO, for example, are protected by law, and the DPO is subject to confidentiality obligations. However, these confidentiality obligations are not necessarily transferred to the role of the CISO. In addition, there is an ongoing legal discussion regarding the guarantor obligations of the CISO or the compliance officer. This does not apply to the DPO. In the worst case, these roles being held by the same person can result in a severe conflict of interest; for this reason, this decision should be thoroughly analyzed and evaluated.
- depending on the size and area of focus of the company/organization and the specific scope of the ISMS, combining the roles of DPO and CISO can also generate synergies that would not exist if the roles were held by separate individuals (in terms of the flow of information, overview and design of TOMs, etc.). In each case, however, it must be carefully assessed whether the candidates in question have the necessary professional and personal qualifications and whether they can handle the workload in both areas. Additionally, a careful assessment must be conducted according to the process previously laid out in this document to determine whether potential conflicts of interest are 'manageable' and whether they will cause severe hindrances to the person carrying out one or both functions.
- another example of a potential conflict of interest between the DPO and CISO involves the collection and analysis of communication and log data. While the DPO is generally only permitted to collect and analyze personal/personally identifiable data under very specific circumstances and for very specific purposes, the CISO's aim is to make the best possible use of technical measures in an effort to increase the level of security (preventative protection) and identify and analyze potentially damaging incidents (detective protection).

The organization must ensure that everyone involved in the process has the appropriate training, education, and/or experience to give them the skills required for the job. The organization must prove that the employees have gained these skills, e.g., by adding training certificates to the educational background section of the respective employees' personnel files (see Clause 7.2 d).

- ISO/IEC 27001:2013 provides a rough framework for the security organization at companies (e.g., top management, risk owner, auditor); however, it does not describe in detail how roles and responsibilities should be allocated in practice.
- for roles required within the ISMS, it has proven beneficial to select employees who already have an inherent connection with information security and/or who have sufficient intrinsic motivation. In addition to the necessary professional expertise, these employees must have appropriate social skills; without proper communication, integrity, objective persuasiveness, and conflict management skills, they will not be able to handle the tasks that arise about implementing the information security strategy and the (sometimes unpleasant or unpopular) decisions associated with it.
- examples of possible organizational structures in the context of information security can be found in 'COBIT 5 for Information Security' (Appendix C), BSI Standard 100-2 – IT Baseline Protection, and other sources. They describe the roles and responsibilities of the CISO, the steering committee, the information security manager, the roles in the risk management process, and the roles of the specialized data owners.

8 See Clause 6.1.2 c and Control A.8.1.2 'Ownership of Assets.'
9 CISO: Chief information security officer
10 CIO: Chief information officer

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- proof of qualifications (Clause 7.2 d)

Additionally, the following documents have proven useful in practice:

- descriptions of roles/job descriptions
- design of strategic and operational partnership between DPO and CISO

References

ISO/IEC 27001:2013 – Clauses 5.3, 7.1 and 7.2
COBIT 5 for Information Security
BSI Standard 100-2 – IT Baseline Protection

3.6 Risk Management[11]

Generally speaking, risk management allows us to analyze anything that could happen, as well as the potential impact of these occurrences, *before* making a decision as to what should be done and when in order to prevent potential harm. The goal is to reduce the identified risks to an acceptable level; the individuals responsible in a given context (and sometimes even in a given situation) have to decide how *acceptable* is defined here. A decision also has to be made regarding how the identified and assessed risks should be dealt with.

Risk management is a comprehensive process within a management system; in an ISMS, it is intended to contribute to the systematic identification, assessment, and transparent presentation of risks in the context of information security and to ensure an *acceptable*/long-term improvement in the *level of security* within the scope of the ISMS.

The specific objectives of risk management in the context of information security are:

- early identification and elimination of information security risks
- establishing consistent assessment methods for identified risks
- clear assignment of responsibilities when dealing with risks
- clear, standardized documentation of risks, including their assessment
- efficient treatment of risks[12]

Success factors for practical implementation

How do risks develop?

In the context of information security, risks are often an inherent consequence of using IT systems and (new) IT technologies. In accordance with ISO/IEC 27001:2013, information security must always be considered from a holistic perspective – this means that there are further sources of risk to an organization's information/data, and they can develop because of the following factors:

- the exchange of data within and outside of the organization
- changes to internal organization and cooperation (particularly at large companies)
- (existing) systems and applications that cannot be updated or replaced
- cooperation with external partners/service providers
- remote access to the company network (by partner companies or manufacturers, for example)
- natural phenomena/natural disasters
- sabotage and white-collar crime
- humans as a risk factor (e.g., social engineering)
- using new systems and technologies (cloud and mobile devices, etc.)
- entering new markets (geographic or product-based)

All sources of risk and risk factors should be considered, but each organization has to define its own areas of focus in risk management based on its field of business and the internal and external requirements that arise in that field.

- risks can only be managed efficiently if the risk exposure and environment of the business field in question are first analyzed. In order to know where exactly to look for risks, you first have to know which areas of risk generally exist and assess them accordingly. A good starting point for this process would be a process map or a situation analysis (see Chapter *3.1 Context of the Organization*).
- ISO/IEC 27005:2011 can be consulted when formulating and designing the risk assessment process. In addition to the detailed main section, the appendices contain useful tips for the implementation.

11 This chapter deals exclusively with risk management in the context of information security.
12 E.g., by updating the security strategy or implementing appropriate security measures.

How are risks identified and assessed?

Before the identification and treatment of risks can begin, the general risk assessment process and the risk acceptance criteria applicable throughout the company/ISMS must be defined in consultation with top management (if the process and criteria could not or did not have to be adopted from a higher level of risk management).[13]

The risk assessment process includes the following:

- Methods for identifying risks
- Criteria for assessing risks
- Criteria for risk acceptance

Methods for identifying risks

The identification of relevant risks generally requires the perspectives of multiple stakeholders/departments to be considered and merged. Various techniques and methods can be used as tools here, including:[14]

- Interviews
- Scenario analysis/'what-if' analysis
- Brainstorming
- Business impact analysis (BIA)
- Checklists
- Delphi method
- STRIDE threat model (Microsoft)

Example:

The people involved in risk analysis for a new e-commerce web application discuss the various risk aspects of the process. The software developer sees a few vulnerabilities in the programming language chosen for the process; resolving them would require a solution like (automated) code reviews. The IT administrator expresses his concerns regarding the planned maintenance of the system by external service providers and the access to the company network that they would need to be granted. The data protection officer raises the issue of properly protecting personal data and requests a list of the technical and organizational measures necessary to meet the requirements of Section 9, Annex 1 of the German Federal Data Protection Act (BDSG). The information security officer, on the other hand, sees the scope of the project (impact of availability restrictions or a data leak) and consequently requests a penetration test prior to the go-live.

- you won't find this example in a textbook, but it shows that risk analysis can also involve drawing up (counter-) measures directly.
- if an organization's risk management process is highly dynamic, drawing up (counter-) measures directly can help to ensure a rapid response to risk. However, if the risk management process is not very dynamic, the organization can purposely avoid drawing up (counter-) measures right away to allow for a complete/comprehensive analysis; further activities can be defined at the company's own pace as a next step.
- a risk management process that is 'compact' or 'dynamic' means that options for treatment are discussed and selected swiftly; the risk here is that, overall, the process will be reactionary and focused on measures, which could potentially result in the risk analysis being missed out.
- in that sense, the best approach should always be selected based on the size and scope of the organization or the specific project.

Criteria for assessing risks

The criteria for assessing risks should be phrased in such a way that they can be used to cover the widest possible variety of risk types/categories. The specific risk management process can be designed using a point-score model or a catalog of qualitative parameters.

- from a practical perspective, it is recommended to provide a set of questions tailored to the organization's field of business in addition to standard criteria (such as the level of protection required for confidentiality/integrity/availability, supported business processes, number of users, etc.). This set of questions can be expanded on a case-by-case basis.
- assessing the probability of occurrence is extremely challenging in practice. In addition to 'looking back' (empirical values, comparable results at other organizations, KPIs, statistics, etc.), it is also extremely important here to 'look forward' in order to consider previously unidentified insights and developments already on the horizon (the emergence of new technologies, for example, or changes to hazardous situations)[15]. Or, to put it another way: "In risk management, success depends on preparation."[16]

13 ISO 31000 describes these activities in Clause *5.3 'Establishing the Context.'*

14 See: IEC 31010:2009 – Annex B – Risk Assessment Techniques.

15 Through APTs or zero-day vulnerabilities, for example.

16 Based on a saying by Confucius, Chinese philosopher, 551 B.C.E. – 479 B.C.E.

Risk acceptance criteria

Defining risk acceptance criteria is a vital step in the risk management process, because it is the only way for the organization to experience the full benefits of the process; it prevents the organization from having to invest the same level of funding and resources in handling all identified and analyzed risks.

- risk acceptance criteria can be defined in terms of acceptance levels based on the qualitative and/or quantitative potential for damage (e.g., non-compliance, financial harm, damage to reputation, etc.).
- risk acceptance criteria can encompass multiple threshold values. Each threshold level can be tied to a specific level of the hierarchy/management so that the acceptance of risks above a certain level can only be handled by the managers appointed within this level.
- for purposes of improved comparability and reproducibility, qualitative damage levels can be converted to (financial) values. These values can generally only be approximate, however.
- for small and medium-sized companies in particular, it may be recommendable to start the risk assessment process with a simplified model and then enhance it step by step. For example, in the first step, risks can be compiled and initially evaluated without a completely fleshed-out model and in cooperation with the experts in the IT department(s). Risk acceptance criteria can be derived from the results step by step and then translated into formal criteria at a later point, upon approval from company management.
- risk acceptance criteria should be defined with care and foresight to ensure that they are in line with the company's attitude toward risk[17] (neither too high nor too low) and that they safeguard the efficiency and effectiveness of the ISMS by allowing risks to be comprehensively identified and consistently treated in accordance with how they have been assessed (not all risks can be given top priority).
- in practice, it would be impossible to implement a risk management system that is completely comprehensive, that detects and analyzes in detail all information security risks in all areas of the company at all times – the same way that it would be impossible and impractical to operate all IT systems with the same level of security. An 'appropriately high' level of security for certain components and processes simultaneously means an 'appropriately low' level of security for other components and processes. The trick is drawing this distinction; it requires sufficient experience and the proper methods and assessment criteria.

Once the risk assessment method has been defined, the steps of the risk management process follow in order:

1. Risk identification
2. Risk analysis
3. Risk evaluation/assessment
4. Risk treatment

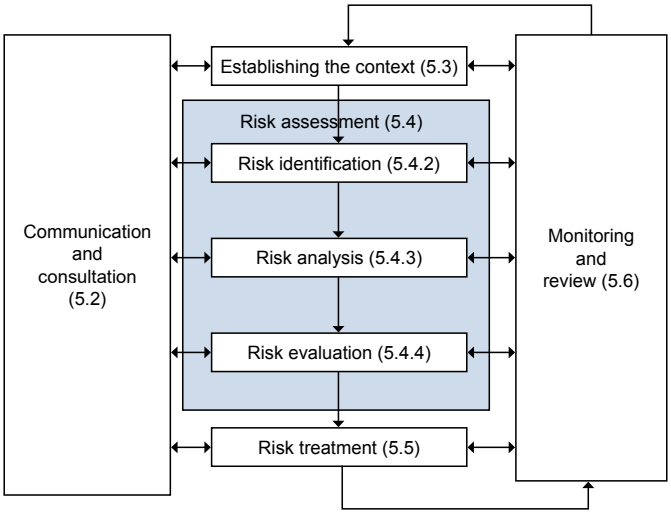


Figure 3: Risk management process in accordance with ISO 31000[18]

Step 1: Risk identification

The risk identification process is always based on information within the scope of the ISMS (see Clause 6.1.2 c).

The following scenarios are examples of how specific risks might be identified:

- audits
  - Audits show that the relevant departments are not properly implementing security standards or existing best practices, or that the relevant systems are not in line with these standards/practices.
  - Naturally, a prerequisite is that audits have been conducted in the first place (see Chapter *3.12 Internal Audit*), and that the audit process includes a clear approach to dealing with the findings of the audit (documentation of findings, handover of findings to the audited department, etc.).
- risk analysis
  - Explicit risk analysis and assessments can be specifically conducted for business-critical processes, applications, and systems; these analyses and assessments can be used to make clear statements regarding the risk situation and risk exposure of the affected processes, applications, and systems.

17 The greater the level of risk a company is willing to accept, the more flexibility and business potential it generally has.

18 1See ISO 31000.

  - In the context of project management, risk analysis (each with an appropriate scope) should be mandatory.
- operations
  - Depending on the risk management process selected, insight gained during 'normal' operations may bring to light previously unidentified risks that should/must be (swiftly) reported to the risk management team upon assessment by the employees/team of experts responsible for the subject.
- security incidents
  - Security incidents (however they are defined) can allow for the identification of previously unknown risks on the one hand; the incident makes these risks 'visible,' so to speak. On the other hand, risks that are already known but have not been sufficiently dealt with, or risks that were accepted up to this point, may materialize (e.g., because of active exploitation of a known vulnerability by an attacker or the failure of a system due to insufficient technical dimensioning).

Step 2: Risk analysis

When analyzing identified risk, the probability of occurrence and the possible impact if the risk occurs should be clearly determined and presented to decision-makers in a comprehensible way.

- when determining how the description of the impact should be phrased, the focus should be on the impact on business processes and the business in general rather than on technical details.
- standardized assessment matrices can be used for risk analysis where, depending on the organization and the specific case, it may make more sense to use matrices with an even number of columns (e.g., 4x4). Matrices with an odd number of columns/rows (e.g., 3x3 or 5x5) carry the risk of the decision more frequently 'landing in the middle'.

Step 3: Risk evaluation/assessment

The (final) decision on how to treat identified risks should lie with the owner of the respective risk, as the owner can best assess the impact of the risk materializing and is ultimately responsible for the business process(es) affected by the risk. Generally, the risk owner also makes decisions regarding the allocation of resources (e.g., financial resources):

- at this point, the importance of the identification and definition of the risk owner for the entire risk management process has been made clear.
- In practice, the role of risk owner should be held by the relevant managers at the company (e.g., board of directors, CEOs, managing directors, team leaders, division heads or department heads). For projects, the project manager is generally the risk owner – at least for project-specific risks.

Step 4: Risk treatment

The way risks are treated depends on the given organization's attitude toward risk or risk appetite. The models in ISO/IEC 27005:2011 are a good starting point for modeling risk treatment options in the context of information security.[19]

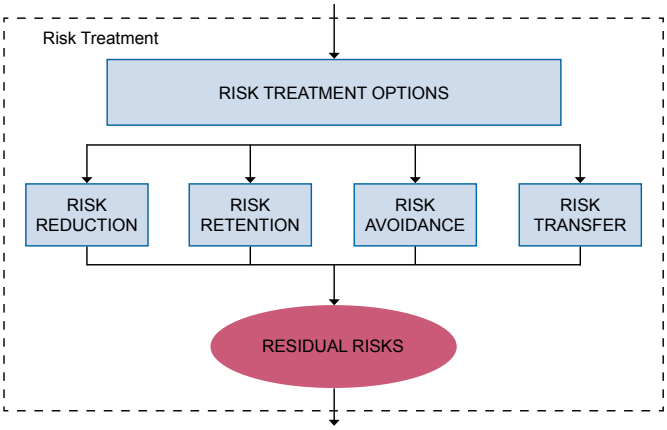


Figure 4: Risk treatment options in accordance with ISO/IEC 27005[20]

- risk treatment measures can be drawn from practically any source, but they must be in line with Appendix A of the standard and the SoA of the ISMS.
- risks must be assigned to the appropriate risk owner. Without dedicated owners, it will be difficult to make a 'correct' assessment or ensure successful long-term treatment of identified risks.
- the risk owner is generally the authority that bears responsibility for the financial impact of the risk if it materializes. In many cases, this is the process owner, but it might also be upper management, depending on the impact and risk assessment.
- even if the risks are caused by IT systems, for example, the affected business areas ultimately suffer the effects. So, even though the respective[21] IT department is responsible for the treatment of (IT) risks, the departments that are affected by the risk and that make decisions regarding the allocation of resources are still the risk owners and are still fully accountable.

19 See Clause 9 of ISO/IEC 27005:2009 – 'Information security risk treatment.'
20 See ISO/IEC 27005.
21 This also includes specialized departments and software development departments that might be located outside of the IT department, that are responsible for their own IT risks, and that are responsible for their own risk treatment.

- the risk identification process and the process of identifying the associated risk owner can be carried out separately/at different times.

How are risks documented?

- it is recommended to keep the results of all risk assessments in a central location, such as a risk register. The standard does not require this, but it can be helpful in evaluating and managing identified risks and their status. Depending on the size of the organization, tools with a diverse range of functions may be required (number of risks, number of users, authorization concept, multitenancy, online availability, evaluation options, etc.).
- the standard does not require a central risk register. However, it does require the information security risk assessment process to produce consistent, valid, comparable and reproducible results (see Clause 6.1.2 b). Consequently, depending on the nature and use of the tools implemented, setting up a register could be a logical step.
- the risk register generally contains sensitive and (strictly) confidential information, so an appropriate role- and permission-based concept for data access should be drawn up and implemented.

General recommendations

- if a higher-level risk management system is already in place at the company or group of companies, the IS risk management system should be integrated into it (e.g., as a component of operational risk management).
- if possible, risk management should be process-oriented rather than emphasizing the individual assets. This ensures that risks and threats are formulated in the most (business) process-oriented way possible, which makes them easier for the risk owners (generally also the process owners) to understand. It also allows the potential (damaging) impacts to be communicated very precisely.
- the process model for implementing projects at the company should be adapted/expanded to ensure that risk analysis and assessment are carried out (at varying levels of intensity depending on the nature and scope of the project). The project team must document the results of the analysis and – depending on how risk management is structured – risks that exceed a defined threshold must be passed on to another level of the hierarchy. There must be a formal, documented handover of risk to the risk owner if there are no measures in place or if the risk is accepted.
- for (extensive) changes to processes, applications, or systems, it is also recommendable to make risk analyses and assessments an obligatory component of change management.
- if non-conformities or vulnerabilities are identified (by monitoring or another operational IT process such as change, problem, or incident management, for example) that cannot be resolved at all or within a reasonable time frame during normal operations, they must be assessed as part of the risk management process and treated by the risk owner.
- risk analyses and assessments always require the specialized expertise of the respective process owner. The organization's IS officers can provide support for the process and can identify and assess risks during interviews or workshops, for example. Another approach involves the use of surveys/self-assessments. Depending on the method selected, these self-assessments might also receive an additional review from a second pair of eyes. The important thing here is that a formal, pragmatic process is in place that provides optimal support for the departments and project managers and simultaneously ensures that risks are identified at an early stage and dealt with appropriately.
- BSI Standard 100-3 – Risk Analysis Based on IT Baseline Protection provides a few jumping-off points for using the threats listed in the IT Baseline Protection Catalogs to conduct a risk analysis for data processing. However, the BSI approach requires that the steps in the IT baseline protection method be carried out first (including information network, structural analysis, determining protection requirements, modeling, basic security check, supplementary security analysis) before a decision can be made regarding the target objects for which a risk analysis will be conducted and the objects for which one is not required.
- in the context of an ISMS, the commodity to be protected is always the information itself. It is the job of the responsible authority in each case (company management, executives, process owners) to assess this commodity in terms of its value to the company/the respective process. In this way, the information commodity becomes an information asset. The job of the risk owner is to establish appropriate, effective, and efficient TOMs in all steps of the process. The ISMS managers are 'watchdogs' for the implementation of the information security strategy, and among other things, they are responsible for truthful reporting on risk exposure and security incidents.

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- risk assessment process (Clause 6.1.2)
- risk treatment process (Clause 6.1.3)
- records and results of risk assessments/risk analyses (Clause 8.2)
- records and results of risk treatments (Clause 8.3)

Additionally, the following documents have proven useful in practice:

- records and results of risk assessments and risk analyses

References

ISO/IEC 27001:2013 – Clauses 6.1, 8.2, 8.3
ISO/IEC 27005
ISO 31000
COBIT 5 for Information Security,
BSI Standards 100-2 and 100-3

3.7 Performance Monitoring & KPIs[22]

A series of provisions (i.e. requirements) are defined in the context of the ISMS, including information security objectives and guidelines/concepts for implementing them in practice. It is expected that compliance with these provisions will be continuously monitored.

Key performance indicators

Specific indicators are used in practice to continuously monitor the effectiveness and efficiency of the ISMS processes and established measures. They provide information about the performance of the entire ISMS and serve as a catalyst for management to get involved when necessary.

This means assessing the current situation compared to the desired situation as laid out in the provisions and to intervene in a corrective capacity as required. These performance indicators are aggregated in terms of the company objectives to be achieved, legal regulations, and protection requirements. The aggregated performance indicators are known as key performance indicators (KPIs).

KPIs are both important and beneficial because they make it possible to make general statements about the security system. They provide management with a transparent, comprehensible basis for making well-founded decisions governing information security. KPIs can uncover indicators of (new) risks and/or changes within the risk landscape, as well as non-conformities in terms of the implementation of security provisions and guidelines.

Success factors for practical implementation

Performance indicators are only useful for illustrating the current situation and managing it if they meet certain requirements. The literature on the subject cites numerous quality criteria for performance indicators: The report 'Information Security Metrics – State of the Art'[23] is a good starting point; it was created by the Swedish Civil Contingencies Agency (Swedish: MSB) as part of the research project Controlled Information Security (COINS).

- all performance indicators must be measurable, reproducible, and comparable, both along the time axis and across industries or at least across the organization.
- indicators must be systematically structured and based on appropriate, sound statistical/mathematical foundations with reliable measurements in a sufficient scope.
- the indicators must be up-to-date and reflect current information. The frequency of data collection and the duration of processing before the data is presented to management should facilitate control of the system – like the indicators on the dashboard of a car, they show the 'driver' of the system whether all important parameters are within the desired and appropriate range.
- performance indicators must be relevant to the information security management objectives, and they must allow for corrective intervention and provide practical support for the decision-making process.
- indicators should be selected based on risk, and they should balance the efficiency of data collection with the significance and usefulness of the data for the decision-making process.
- the KPIs selected should allow for an assessment of the entire ISMS. It is insufficient to measure only certain aspects or indicators. Rather, they must be part of a logical whole that reflects the performance of the entire ISMS.
- performance indicators can also be used to assess and manage service provider relationships – as part of a contract, for instance, or in a (security) SLA.

22 KPI: Key performance indicator

23 Barabanov, R.: Information Security Metrics – State of the Art. DSV Report Series No. 11 – 007, 2011.

Relevant KPIs for the ISMS

There are many sources for performance indicators in information security; they offer an enormous selection. COBIT 5 for Information Security[24], the CIS Security Metrics[25], and the Performance Measurement Guide for Information Security[26] are just a few examples. Specific KPIs should be selected based on the circumstances at the organization, meet the already described criteria and be continuously optimized.

The following are generalized examples of these sorts of performance indicators:

- **integrating information security/IT security into projects**
  - Proportion of projects involving IT security requirements in relation to the total number of projects
  - Proportion of projects with IT security shortfalls at go-live with and without formal risk evaluation during the project phase in relation to the total number of projects
- **deviations from IT security and architecture standards**
  - Number and development of approved deviations from internal requirements over time
  - Development of detected, unapproved deviations from the required standard over time
  - Proportion of detected deviations that were resolved in relation to deviations approved after the fact
- **incident response/problem management**
  - Proportion of the security loopholes that cannot be closed (deviation from the standard) in relation to the total number of deviations detected
  - Proportion of security loopholes that were successfully closed in the pre-defined time in relation to the total number of known security loopholes
- **asset ownership**
  - Number of information assets that are assigned to an owner in relation to the total number of information assets as a percentage

Using metrics

An indicator is closely tied to a protective measure (technical or organizational) to measure its effectiveness based on defined parameters. An indicator has a defined normal range for regular operations with one or more ranges of tolerance, as well as threshold values for alerts. Each indicator can have a specific cycle including a predefined countermeasure so that the person managing it is not burdened with the details. If the measured value is outside of the normal range but still within tolerance, the countermeasure is sufficiently implemented. If the countermeasure is ineffective and the threshold value is exceeded or if there are regular fluctuations within tolerance of that value, an alert is triggered.

Example:

Just like in a car, the driver isn't notified every time a sensor reading from the engine deviates from the normal, unless there is a risk that engine performance or integrity could suffer. A warning light comes on in these cases. This allows the driver to draw his or her own conclusions and make a risk-based decision about the continued use of the vehicle.

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- documentation of the measurement structure for all KPIs. This answers the following questions:
  - How are the metrics defined in detail?
  - What was measured and evaluated?
  - Which methods were used for measurement, analysis, and evaluation, and do they lead to reproducible results?
  - When were measurements conducted, and by whom?
  - When were analyses and evaluations conducted, and by whom?
- **results of measurements and the derived management reports for escalation**

Additionally, the following documents have proven useful in practice:

- **all records and evidence that prove effectiveness.**

References

ISO/IEC 27001:2013 – Clause 9.1
ISO/IEC 27004:2009 – Clauses 5, 6, 7, 8, 9, 10 and Annex A
COBIT 5 for Information Security

3.8 Documentation

In the context of documentation, a primary requirement is that the following aspects are regulated (at least) for ISMS documentation within the management system:

- documents must be created, updated, approved and, if necessary, published according to a defined workflow.
- the documents must be clearly labeled, e.g., title, date, author, version, storage location, performance and suitability test (QA), and final approval.

24 ISACA: COBIT 5 for Information Security, 2012.
25 The Center for Internet Security: The CIS Security Metrics, 2010.
26 Chew, E.; Swanson, M.; Stine, K.; Bartol, N.; Brown, A.; Robinson, W.: Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Revision 1, 2008.

- classification of documents/their contents in terms of confidentiality
- creation of sufficient records with relevant content as part of operational tasks to ensure transparency and reproducibility

The content and degree of detail that the standard requires in documents depends in part on the selected scope of the ISMS, the size of the organization, the technologies utilized, and the organizational structure; for this reason, these factors differ from organization to organization.

The number and type of documents can also vary. From a practical perspective, it can be a good idea for a given organization to create a set of (numerous) individual documents and maintain them granularly. For other organizations, on the other hand, it may make more sense to use a central storage medium that can be accessed from anywhere in the organization. In practice, this can mean using a wiki or another online system as the basis for documentation.

If no specific documents are required, the standard ISO/IEC 27001:2013 uses the term 'documented information' in connection with documentation and records. In this case, it is left up to the company to decide what types of documents should be used to manage this information; the term 'document' can comprise any number of formats.

The documentation required within the ISMS must be continuously monitored to ensure the following:

- availability and suitability for the intended use, regardless of time and location
- appropriate protection, e.g., from loss of confidentiality, improper use, or unauthorized manipulation/loss of integrity

Success factors for practical implementation

In practice, a document guideline can support the process of meeting document management requirements. However, the quantity of documentation is not decisive in ensuring the success of implementation; quality, acceptance, availability, and efficient document management are what matters.

Practical aspects of assessing document quality and document management can be drawn from the following questions:

- how familiar are employees with the content, and how do the affected parties model the requirements of the documents in their day-to-day work?
- who knows where and on what media the latest documents are stored?
- is the content target group-oriented and clearly phrased?
- how easy is it for employees to understand the content of the documents and to implement it in their own work environment? What kind of requests are there?
- are documents updated regularly/upon request? How well do the update and approval processes for the documents work?
- are there dedicated document owners for each document?

Documentation requirements

The following minimum documentation requirements always apply according to ISO/IEC 27001:2013 (Clauses 4-10):

- Scope of the ISMS (Clause 4.3
- Information security policy (Clause 5.2 e)
- Description of the risk assessment process (Clause 6.1.2)
- Description of the risk treatment process (Clause 6.1.3)
- Statement of applicability (Clause 6.1.3 d)
- Information security risk treatment plan (Clause 6.1.3 e)
- Information security objectives (Clause 6.2)
- Evidence of competence (Clause 7.2 d)
- Proof of proper execution of the ISMS processes (Clause 8.1)[27]
- Results of the information security risk assessment, (Clause 8.2)
- Results of the information security treatment (Clause 8.3)
- Evidence of the monitoring and measurement results of the ISMS (Clause 9.1)
- Evidence of the audit program(s) and the audit results (Clause 9.2)
- Evidence of the results of management reviews (Clause 9.3)
- Evidence of the nature of the nonconformities and any subsequent actions taken (Clause 10.1 f)
- Evidence of the results of any corrective action (Clause 10.1 g)

Moreover, the organization must determine for itself which documentation and records are necessary in addition to those required by the standard to 'establish sufficient trust that the processes will be carried out as planned' (see Clause 8.1).

27 In this context, the standard refers to 'documented information in the necessary scope.'

Added to that are the documents and records from Annex A, if these measures are applicable in accordance with the statement of applicability.

References

ISO/IEC 27001:2013

3.9 Communication

When operating an ISMS, cooperation with other organizations and departments is required (suppliers, human resources department, legal department, audit, etc.). The primary task of the 'Communication' component is determining and describing the requirements for internal and external communication.

External communication here refers to communication with (external) stakeholders and other organizations (see the situation analysis in Chapter *3.1 Context of the Organization*). Internal communication refers to the need for communication within the management system and within the organization – e.g., with internal stakeholders such as the board of directors, executives, and employees.

An analysis should be conducted to determine which information (Clause 7.4 a) has to be communicated to whom (Clause 7.4 c) by whom (Clause 7.4 d) in the context of the ISMS. Moreover, it must be determined when this information has to be communicated (Clause 7.4 b) and via which communication channels/processes (Clause 7.4 e).

Ideally, the results of the analysis will be summarized in a communication plan. This is generally developed as part of a formal process with five specific steps:

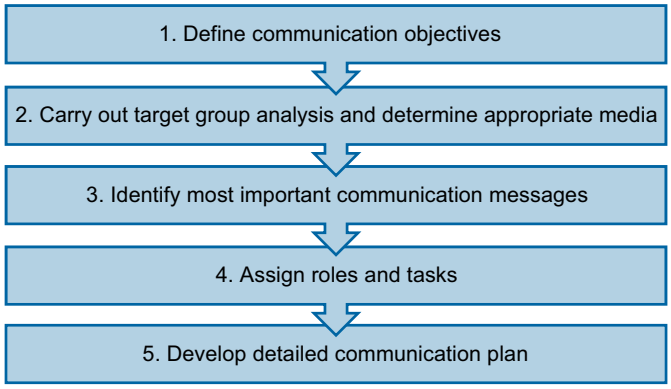


Figure 5: Developing a communication plan

- in the interest of efficiency, process and communication interfaces should be clearly defined and integrated into organizational and operational processes. There must be clear rules regarding which information has to be sent to whom by whom at what time – in the context of change or incident management, for example.
- the standard requires the organization to define internal and external communication in the context of the ISMS. It does not explicitly require this to occur as part of an analysis. However, the practical advantage of an analysis is that it can be used to clearly identify the requirements for a custom-tailored communication structure.
- when the communication matrix is complete, it generally becomes clear that numerous interfaces between communication partners and/or departments already exist. Identifying these interfaces is an important factor in successfully shaping efficient communication within the organization in the context of the ISMS. It can be a good idea to integrate the IS communication plan into an overarching communication plan.
- a platform for communication between all levels of the organization should be provided so that a range of different target groups have access to the comprehensive security information in the ISMS. Collaboration platforms for improved communication/reporting can include the intranet, Confluence, wikis, etc.

Success factors for practical implementation

A communication plan, also known as a communication matrix, might look like this:

Internal Communication				
Reason for Communication	*Initiator*	*Recipient*	*Frequency*	*Medium*
Management review	CISO	Top management	Annually	Management report according to template via e-mail + presentation
Reporting	CISO	Top management	Quarterly	KPI report according to template via e-mail + presentation
Awareness training	CISO	All employees within the scope	Annually	Training (classroom/online)
IS newsletter	CISO	All employees within the scope	Quarterly, and on a case-by-case basis if an acute threat occurs	E-mail
Risk management	CISO	Top management	Quarterly, on a case-by-case basis if an acute threat occurs, on a project basis	Balanced scorecard report, by e-mail if required
Security incident	Support	CISO *(possibly others, in accordance with SIRP)*	Case-by-case basis	Escalation in accordance with SIRP (security incident response process)
Security incident	CISO	Top management	Case-by-case basis	E-mail, possibly verbally
Security incident involving personal data	CISO	Data protection officer	Case-by-case basis	E-mail, possibly also by telephone or verbally
Compliance-related security incident	CISO	Legal advisory department	Case-by-case basis	E-mail, possibly also by telephone or verbally
External Communication				
Reason for Communication	*Initiator*	*Recipient*	*Frequency*	*Medium*
Operational service provider report	Operational service provider	CISO	Quarterly	SLA report according to template via e-mail
Externally commissioned CERT/ vulnerability analysis	CERT	CISO/head of IT	Weekly/case-by-case basis	Report in accordance with contract by e-mail
Security incident	CISO, possibly top management	Affected customers/partners	Case-by-case basis	In accordance with SIRP, on the website, by mail, e-mail, by telephone
Security incident of a criminal nature	CISO	Law enforcement agencies	Case-by-case basis	In accordance with SIRP

Documentation requirements

ISO/IEC 27001:2013 does not include any specific documentation requirements for the ISMS in the context of communication.

Additionally, the following documents have proven useful in practice:

- procedures for internal and external communication
- communication matrix
- communication plan

References

ISO/IEC 27001:2013 – Clause 7.4

3.10 Competence and Awareness

"Information security means using firewalls and anti-virus programs." – This is one of the biggest misinterpretations of the concept of information security, and it can put a company's information and IT systems at grave risk. Numerous security-relevant events and security incidents can occur during operations because of 'a lack of accountability,' 'a lack of processes,' or 'a lack of training and/or awareness among employees.'

Obviously, making employees and executives aware of the issue isn't a magic bullet when it comes to preventing information security-related issues. There is no empirical evidence that the number of security incidents decreases because of awareness campaigns. In fact, the opposite is usually true, because employees tend to report security incidents more frequently as their awareness increases (regardless of whether those numbers include some false reports). In that sense, it is not necessarily a bad thing if the number of security incidents reported goes up. One thing is clear, however: If an employee or manager is not very aware of the applicable security regulations and processes or the specific risks that they face daily, it will be even more difficult to achieve the desired level of security within the company and to ensure transparent communication of the issue.

Creating a robust and balanced level of risk awareness within a company is consequently an essential component of a functional ISMS that generates value for an organization by identifying threats at an early stage, preventing security incidents, and eliminating the labor that would have been required to deal with these materialized threats.

However, security awareness isn't something that is created out of thin air; it requires active support and effort on the company's part (in the form of awareness campaigns), and it must address the following points (see Clause 7.3):

- it must be ensured that the intended audience for the guidelines (employees, executives, external partners) is aware of the information security policy and the relevant information security guidelines.
- each individual employee's contribution to the effectiveness of the information security guidelines within the scope of the ISMS must stem from materials that are used in the context of an awareness campaign and that can be proven through testing, if necessary.
- consequences of and possible sanctions for non-compliance with security provisions must stem from materials that are used in the context of an awareness campaign.

Success factors for practical implementation

In practice, information security awareness campaigns can generally be broken down into three different phases. First, requirements are assessed, and an awareness campaign is then planned and implemented based on specific potential threats and with a focus on the appropriate target. Information security awareness must be more than just a one-off project; mechanisms must be included in the campaign to ensure that it is sustainable. Methods for assessing the campaign's effectiveness should be considered in advance.

In practice, the following phases have proven useful in security awareness campaigns:

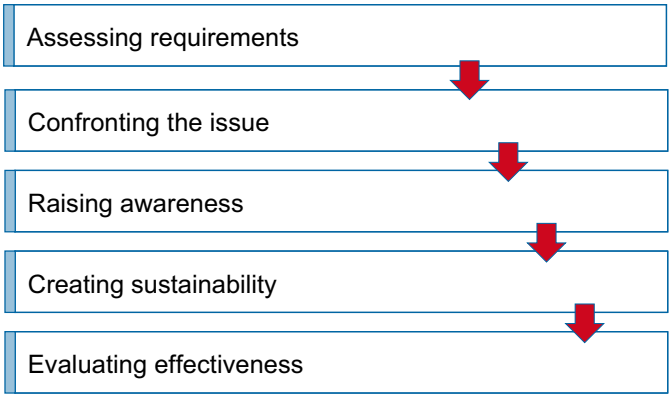


Figure 6: Phase model for security awareness campaigns

Phase 1: Assessing requirements (Based on potential threats)

Successful implementation of security awareness campaigns requires you to know your target group and their needs. For this reason, the first step in any awareness campaign should be to assess requirements.

- raising awareness of security issues is helpful in all areas of the company; however, the scope should be restricted to actual threats and directed toward the appropriate target group.
- awareness campaigns with active participation and participant logs can serve as evidence of the awareness of security provisions among employees of an organization.

Before a company begins planning and defining its awareness campaigns, it should consider each individual threat/risk it faces regarding users. It is not particularly helpful to confront users with threats and scenarios that do not apply to their department.

Phase 2: Confronting the issue

The purpose of the 'confrontation' phase is to attract employees' attention and promote acceptance of Phase 3, the actual process of raising awareness. The best way to handle this is generally to confront employees directly (experiential learning).

- through personal experience, employees become more aware of their own role in safeguarding information security, and generally, they are then grateful for and interested in further training on the subject.

The following is a list of attack simulations that can be used to confront employees with the subject:

- social engineering attacks on employees, such as fake calls aimed at obtaining confidential information (such as passwords) and fake e-mails (e.g., containing a request to enter a password into an online system, supposedly to check the password's strength for an upcoming audit).
- leave manipulated USB flash drives lying around throughout the company (parking lot, meeting room, bathroom, etc.); when used, these drives generate warning messages that are anonymously registered and can be used for evaluation ("I could have been a virus!").
- search the paper recycling bin and wastebaskets for confidential documents ('dumpster diving').

In practice, it has been shown that at most companies, these attack scenarios lead to reported security incidents and usable information that are 'valuable' in this context. The anonymous resolution of the scenarios combined with the explanation of the possible consequences for the company generally serves as a wake-up call to employees, which can be used as a segue into the actual IS campaign ('knowledge transfer').

This 'confrontation' phase can also be conducted passively, such as at the beginning of classroom training, in place of these types of campaigns. Demonstrations might include live hacking sessions, anonymous tests of password strength, or role-playing exercises.

- an essential aspect of this phase is to create a positive starting point for addressing the issue and to communicate with employees on a level playing field. The primary focus of the confrontation phase should always be to meet employees on their current level (Which IS regulations are already in place? How have they been communicated in the past? What sorts of incidents have occurred? Etc.) In addition, get them actively involved in the process.
- it is also important to be clear on the situation at hand and address any existing information gaps. The scope of the activities implemented and information provided must be balanced against the audience's ability to take it all in. This is the only way to ensure that the campaign will have the desired impact and that its audience will not perceive it as too simplistic or too excessive/overblown.

Phase 3: Raising awareness

The actual process of raising awareness should ideally consist of a mix of knowledge transfer, practical demonstrations, and active employee participation. A range of different methods can be used for knowledge transfer purposes (classroom training, e-learning programs, etc.).

Categorizing awareness campaigns into subject areas or strategies as follows has proven effective:

- **physical security/workplace security**
  - What must be kept in mind in terms of physical access to buildings and rooms?
  - How can unauthorized individuals be prevented from gaining access, such as by making fake deliveries or 'piggybacking' (sneaking into the building by joining a group of employees)?
- **data protection**
  - The data protection aspect should highlight the legal requirements, such as data confidentiality and employee obligations.
- **IT security**
  - What needs to be kept in mind when working with IT systems and computers, including dealing with e-mails, surfing the Internet, using removable data media (CDs, USB flash drives), malware protection/tools, etc.?
- **phone calls**
  - What can happen if confidential information or processes are disclosed over the phone?
- **reporting and dealing with security incidents**
  - What are the (central) points of contact?
  - What are some important first steps?

First, target groups that are at high risk (e.g., IT administrators, employees and executives with extensive physical and digital access permissions and information rights, mobile employees, call center employees, or other groups with external contact) must be considered to determine whether they require special training.

Awareness materials should be drawn up and distributed as necessary to support the training process. These materials might include simple or detailed brochures or newsletters with content relevant to the training process, or posters, stickers, or other media that serves as an effective reminder (signs, flyers, videos, etc.).

- ideally, the employees will create these awareness materials themselves as part of the IS campaign. An incentive system can generate additional motivation to participate.

Phase 4: Creating sustainability

One-off awareness campaigns are not enough to change employees' behavior over the long term. Obviously, an extensive initial awareness campaign is important, but only regular repetition of the issue based on a training plan and regular communication of the primary messages during day-to-day operations can ensure lasting awareness. There are many options for raising day-to-day awareness of the issue on a subconscious level, such as:

- publishing the latest news (on the intranet, in the employee newsletter, etc.)
- adding an online quiz on information security to the intranet (possibly including incentives)
- using a screen saver that displays messages about information security

Phase 5: Evaluating effectiveness

During this phase, the level of employee awareness is assessed regularly. The goal is to create greater transparency in terms of the level of employee awareness. The following are possible KPIs:

- number of security incidents resulting from improper conduct in relation to all security incidents
- results of a quiz or test on information security

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- proof of employee competence within the scope of the ISMS (Clause 7.2)

Additionally, the following documents have proven useful in practice:

- **awareness/training concept**
  - What issues are addressed?
  - How are awareness campaigns carried out (e.g., classroom training and/or online training)?
  - How is the content of the information security policy communicated?
- **awareness/training plan**
  - When will each issue be addressed?
  - Are campaigns regularly updated as the standard requires?
- training documents that explain the content of the information security policy clearly and concisely and point out the risks and vulnerabilities in information processing
- proof of participation: Names of the participants, content and date of the awareness campaign

References

ISO/IEC 27001:2013 – Clauses 7.2 and 7.3

3.11 Supplier Relationships

The high degree of standardization and interconnectedness in information processing has fostered the need for a great many external service providers. However, the security risks associated with service providers also have an impact on an organization's own infrastructure. Highly publicized incidents from recent years are proof of this fact; in these cases, security flaws at service providers led to data theft or other security incidents at well-known companies.

The term 'service provider' or 'supplier'

In the standard ISO/IEC 27001:2013, the term 'supplier' covers a broad range of business relationships with external companies and partners. For example, it can include relationships in logistics, with utilities, IT (outsourcing) providers, facility management, cleaning services, and many others.

The requirements of ISO/IEC 27001:2013 are focused on various protective measures, such as the creation of guidelines (Clause 15.1.1) and agreeing on contractual provisions with suppliers (Clause 15.1.2), although risks arising from suppliers' ICT infrastructure, supply chains, and other forms of contracting must be considered (Clause 15.1.3). Rules on monitoring (Clause 15.2.1) and change management (Clause 15.2.2) are also required.

ISO/IEC 27036 and other relevant standards

The standard ISO/IEC 27036, 'Information Security for Supplier Relationships,' provides a much more detailed view. It covers the required processes and describes the activities necessary in each process. It is not possible to become certified for this standard, but there is shared terminology that can provide concrete support for implementation.

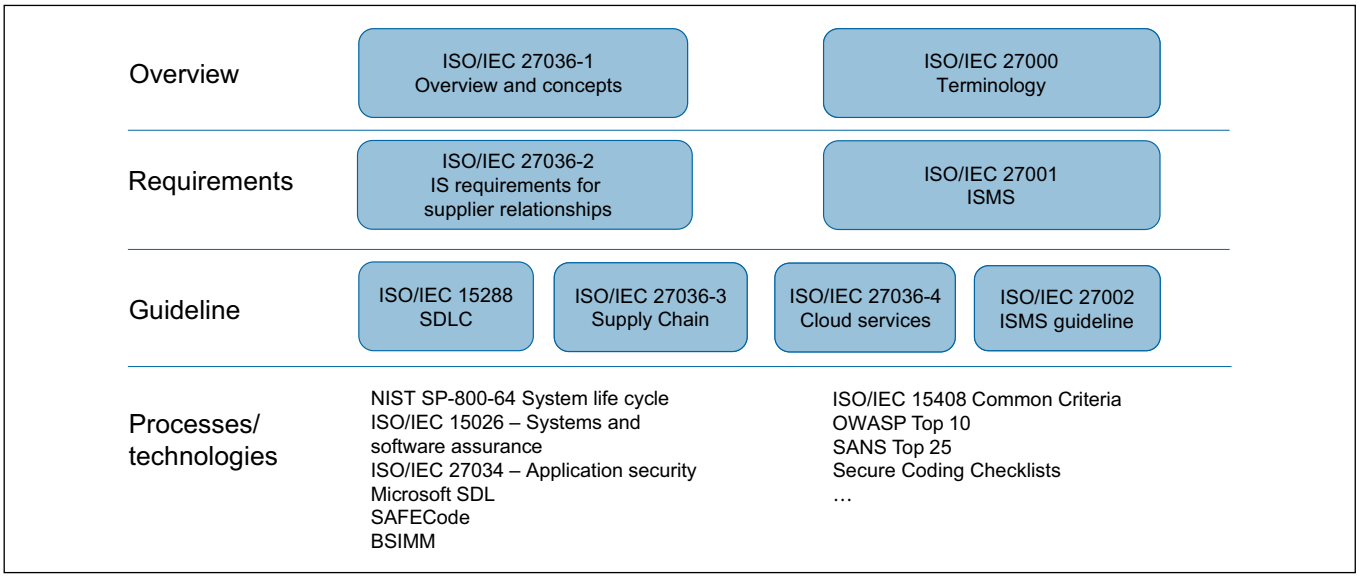


Abbildung 7: IS-Normenübersicht zu Lieferantenbeziehungen

Figure 7 shows an overview of the standards relevant in this context, subdivided into overview, requirements, and guidelines, as well as additional documents that focus on processes and technologies.

In regulated industries, for example, there may be other specific requirements (such as MaRisk AT 9 for German banks) that need to be considered.

Success factors for practical implementation

Comprehensive risk evaluation

It is important to investigate all risks that your organization may face because of cooperating with external service providers. The standard requires all processes outsourced in this way to be clearly defined and controlled over the long term (see Clause 8.1).

ISO/IEC 27036-1 allows supplier relationships to be categorized. It differentiates between:

- supplier relationships for products
- supplier relationships for services
- supply chain for information technology
- cloud computing

Right to audit

The right to audit should be included in every contract.

- standard contracts with cloud service providers generally do not grant this right, however; in these cases, alternatives should be considered, such as the right to access the results of external audits or the provision of certificates, including the scope of each certificate.

Certifications

Customers' demand for information security is increasingly being met by certifications. ISO/IEC 27001, ISO/IEC 27018 for processing personal data in the cloud, and parts of the international standard ISAE 3402 'Assurance Reports on Controls at a Service Organization' are well suited to this purpose.

- in every case, a complete report of the audit and its results is extremely important, as the scope of a given audit and the controls assessed may vary. Potential deviations should still be assessed by the organization commissioning the audit in accordance with that organization's attitude toward risk.
- careful scrutiny must be applied to the hiring of external service providers to handle personal data, especially service providers outside the reach of German or EEA law[28].
- order data processing (ADV) in accordance with Section 11 of the German Federal Data Protection Act (BDSG)[29] also falls under this heading, regardless of where the service provider is located.

Key performance indicators

The following key performance indicators[30] can be used to evaluate information security in relation to external service providers, for instance:

28 EEA: European Economic Area
29 BDSG: Bundesdatenschutzgesetz (German Federal Data Protection Act)
30 Excerpt from McWhirter, Kurt; Gaughan, Ted: The Definitive Guide to IT Service Metrics. IT Governance Publishing, 2012.

- number of service provider relationships that have been subjected to the defined IS supplier process in relation to all service provider relationships
- number of service providers that contractually guarantee IS measures in relation to all service providers
- number of audits at service providers within a year in relation to all service providers
- number of recorded policy violations by suppliers
- number of security incidents caused by service providers during the last reporting period

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- determining the scope, taking into account dependencies of external partners and service providers (Clause 4.3)

Additionally, the following documents have proven useful in practice:

- A.15.1.1 requires the creation of a guideline for service provider relationships. This document should define the requirements resulting from the procurement strategy and all service provider relationships.

References

ISO/IEC 27001:2013 – Clauses 4.3 and 8.1
ISO/IEC 27036-1:2014

3.12 Internal Audit

The primary objectives of internal ISMS audits include monitoring the extent to which the ISMS meets the requirements of the organization, and the requirements of ISO/IEC 27001:2013 (conformity control), and monitoring the implementation and effectiveness of the measures taken (implementation and effectiveness control).

To that end, an audit program must be planned and implemented; it should govern aspects such as frequency, procedure, roles and responsibilities, planning requirements, traceability, and reporting. In addition, a method for dealing with corrective and preventive actions (the measures derived directly from the audits) must be defined, and it must be determined who will follow up to ensure that the measures are implemented.

The audit program is intended to ensure that all the business processes covered by the ISMS (in accordance with the scope) are audited at least once every three years in terms of the applicable provisions and guidelines on information security and in terms of conformity with the ISMS. Evidence of the audit must be provided.

For purposes of the standard, the term 'internal audits' does not refer to internal audits in the narrow sense, although this department may be the one to actually conduct internal audits. In practice, the internal ISMS audits are a primary task of the ISMS officer/CISO, who – in cooperation with an internal audit team or external support, if necessary – plans and manages audits.

Success factors for practical implementation

A distinction can be drawn between two areas when implementing internal audits:

1. The 'audit program'/'audit framework,' which serves as an organizational scaffolding for controlling and monitoring all activities in the context of internal audits and as an interface to other processes in the ISMS.
2. The actual 'audit activities' that include the planning and practical execution of individual internal audits.
   - The purpose of the audit activities is to implement the audit program within the company.
   - It is a good idea to coordinate with the internal auditing department.
   - In larger organizations, it is often recommendable to separate these two departments; an audit team leader is then responsible for the audit program, while a team of auditors carries out the internal audits.
   - It must be ensured that the overall design and operational management of the audit program are optimally tailored toward achieving the IS objectives. In this way, the organization will achieve the best possible return on investment for the resources it puts toward auditing.

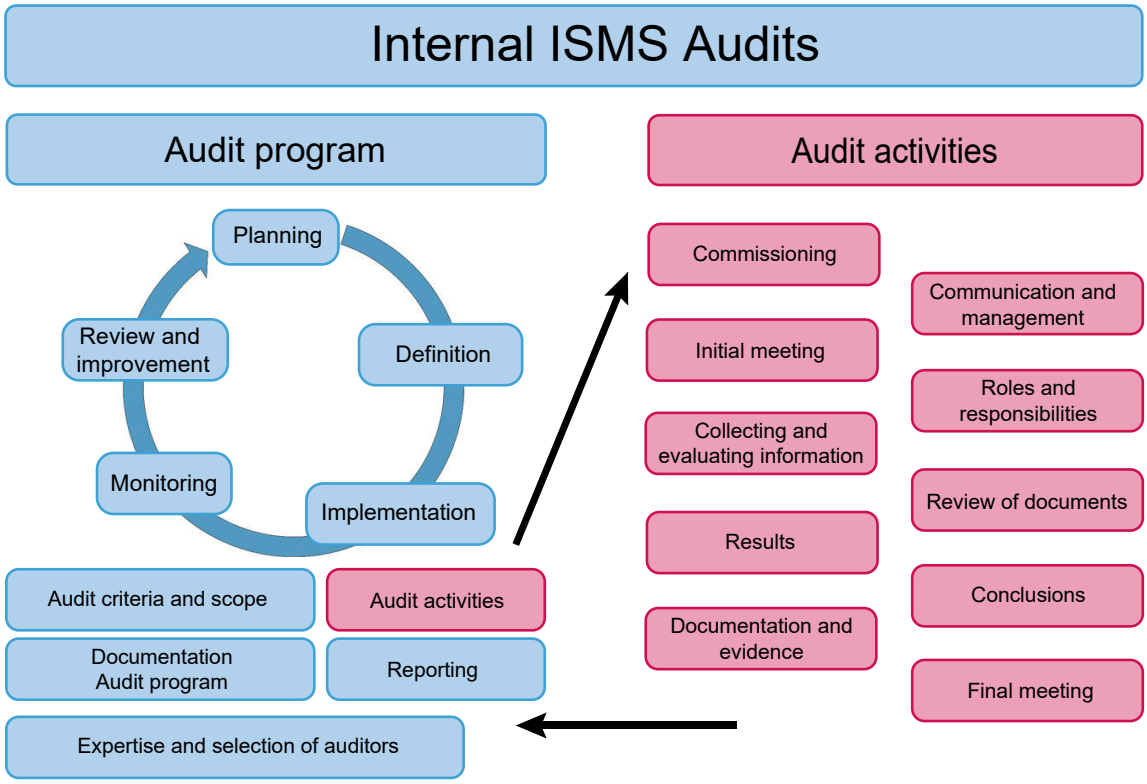


Figure 8: Structure for internal ISMS audits (audit program vs. audit activities)

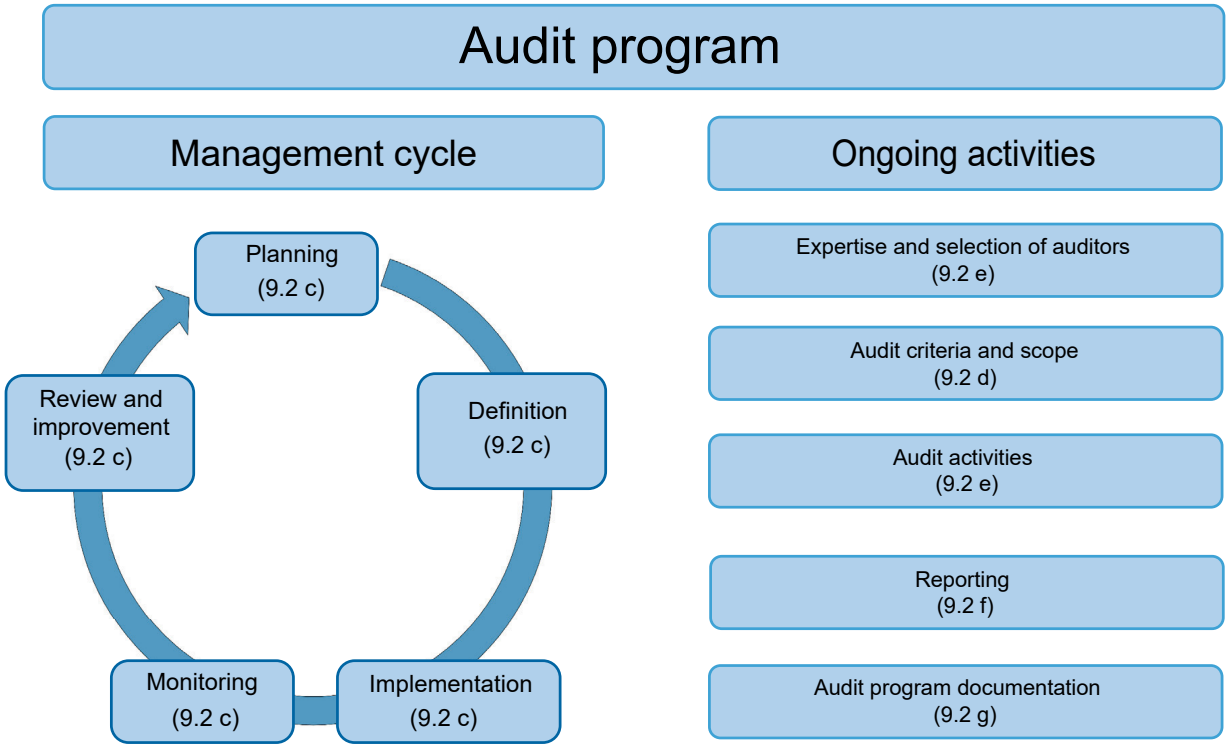


Figure 9: Audit program requirements[31]

31 Citations in refer to Clause 9.2 of the standard ISO/IEC 27001:2013.

The audit program

The audit program is a cyclical process, which includes the sub-processes planning, definition, implementation, monitoring, and review and improvement of the audit program itself.

- the importance of the affected processes (core processes, damage effects, business criticality) and IT systems and the results of previous audits must be considered in the audit program and in risk-based planning of specific audit activities.
- general audit criteria must be defined in the audit program. Depending on the size of the organization, the number of audits conducted, and the desired degree of detail in the audit program, the specific scope of individual audits can also be directly defined here.
- completed audits must be documented and associated information (such as audit reports) must be provided as evidence that the audit program has been implemented.
- management reports with information about the audit program's performance and about the audit activities and their results must be regularly generated.

'Planning' sub-process

The audit program should be based on the respective organization's individual requirements (see Clause 4.2 and 4.3 of the standard and Chapter *3.1 Context of the Organization* in this guideline). Furthermore, the documented objectives of the audit program should make it clear that:

- the audits are based on the established risks,
- the importance of the individual business process has been considered, and
- the audit program covers the scope of the associated ISMS.

'Definition' sub-process

The employees responsible for the audit program must complete the following tasks:

- defining and implementing the audit program
- identifying, assessing, and treating the risks that impact the audit program directly (scarce resources, gaps in auditor qualifications, overly large scope for individual audits, etc.)
- establishing processes for conducting audits
- ascertaining and procuring the necessary resources
- defining the audits and determining the areas and criteria for individual audits
- determining the methods and tools to be used
- selecting the auditors and ensuring that they have the proper qualifications
- ensuring that the audit program documents are always kept up-to-date
- continuous monitoring and improvement of the audit program itself

'Implementation' sub-process

The decisions made during the 'definition' sub-process must be applied in order to implement and execute the audit program.

Whether the objectives and scope for individual audits have already been defined here, depends on the respective design/level of detail of the audit program in question. The objectives and scope of audits are generally based on the individual requirements and required protection level of the affected IT systems.

It is recommended to select the areas to be audited so that they can be audited individually and with a minimum of effort. Other factors for selecting the areas to be audited include the criticality of the business/service processes and the tolerable period between two audits. Naturally, the total of all audited areas (within three years) must be in line with the scope of the ISMS.

'Monitoring' sub-process

In the 'monitoring' sub-process, the audit program itself must be continuously monitored in terms of quality and efficiency. It must be determined whether

- the audit program is still tailored toward the scope of the ISMS and the requirements of the business,
- time and resources are being appropriately allocated,
- the 'right' processes/areas/applications/systems/data are being audited, and
- the depth and nature of the audit is sufficient to meet the objectives.

It is helpful to document the work required for each audit. Since the work required can vary depending on the nature of the IT system and/or the organizational unit involved, this data is gathered in order to better assess the amount of work that will be required for future audits.

When monitoring the performance of the audit team members, it is important to keep an eye on the quality of the audit results. One relevant aspect here is whether the department responsible for an IT system is given transparent, appropriate, and comprehensive recommendations for how to resolve the shortcomings detected by the audit. If the department does not understand the recommendations, perhaps because information is missing or the recommended course of action is inappropriate, this is a sign that the members of the audit team require additional professional or methodological support.

This sub-process also includes collecting and assessing feedback from management, the audited departments/organizational units, the auditors, and other stakeholders.

'Review and improvement' sub-process

In the 'review and improvement' sub-process, the people responsible for the audit program regularly assess whether the stakeholders' expectations are still being met. These assessments are based on information gathered during the 'monitoring' sub-process. The auditors' professional and methodological development must be continuously tracked and managed.[32]

The status of the audit program must be reported to the respective managers. It is also advisable to introduce KPIs here in order to make the overall quality of the audit program and internal audits measurable and comparable. Statements regarding quality, such as 'percentage of strategies accepted by the departments and approved for implementation,' are preferable to statements that only address the time spent, such as 'working time required for each audit.'

Expertise and selection of auditors

- the ISMS auditors selected should deliver the objectivity, expertise, and neutrality that the audit process requires.
- the skills that an internal auditor needs should be described (e.g., in a job description or description of duties).

Planning and conducting audits

Audits identify non-conformities with existing provisions as well as potential, unidentified vulnerabilities and threats.

- the following applies during the audit planning process: An audit cannot be conducted unless it has been specifically commissioned. This means that the actual work should not begin until it is certain that the audit has been commissioned and this fact has been formally communicated. Additionally, the department to be audited should be included in the audit planning process to help determine the scope, the schedule, and the availability of contact persons within the department during the audit, etc.
- (immediate) measures for appropriately dealing with threats should be drafted during the audit, if possible. However, the implementation of these measures must be formally coordinated with the respective service, system, and/or data owners.
- if previously unidentified deficits or risks that are inherent to the process are identified and cannot be dealt with quickly, they must be added to the central risk inventory.
- audit results must be regularly reported to ISMS management, at least in a consolidated form.
- The audit reports must clearly indicate which systems and documents were assessed/inspected and used as a basis for the audits.
- candid communication throughout the course of the audit makes a significant contribution to dispelling reservations within the department being audited, which lowers the risk that employees will withhold information or provide incorrect or distorted information.[33]
- in order to determine whether the measures implemented are appropriate, comprehensive, and effective, the auditor directly surveys the employees primarily responsible for operating and monitoring these measures, reviews the documentation, and/or arranges and assesses practical demonstrations. The auditors require extensive technological expertise and methodological skills for this process. In that sense, it is recommendable to select auditors based on the objectives and content of the audit.
- the responsible levels of management must clarify how the costs of the audit will be handled during the planning process for individual internal audits (i.e., before implementation begins).
- the wrap-up meeting for an audit is the latest point at which the results should be discussed with the audited department, as the department needs to understand and accept the conclusions of the audit and the recommended course of action. The aim should be formal approval of the audit report. Differences of opinion that cannot be resolved must be documented in the report.
- it must be ensured that the relevant information and audit reports are treated confidentially and stored/archived in a location where they are protected from unauthorized access.
- the requirements for internal audits laid out in Clause 9.2 can be met by implementing the recommendations from Clause 6.4 of ISO/IEC 19011:2011 and ISO/IEC 27001:2013. However, it should be noted that the normative requirements in ISO/IEC 27001:2013 are nowhere near as extensive as described in conventional best practices.
- further information regarding internal audits can be found in the ISACA IT Assurance Framework (ITAF). This guidance is geared toward internal IT audits, but logically, it can also be used for internal ISMS audits.[34]

32 See Clauses 7.4, 7.5, and 7.6 of ISO/IEC 19011.

33 See also: 'Communication – The Missing Piece,' ISACA Journal 3/2012 *(http://www.isaca.org/Journal/Past-Issues/2012/Volume-3/Documents/12v3-Communication.pdf).*

34 See *www.isaca.org/itaf*.

Distinction between internal ISMS audits and certification audits

Internal (ISMS) audits are a vital tool in the management system's continuous improvement process. They are used to verify whether the management system meets the organization's own requirements, and to determine where potential for improvement exists. The audit program ensures that all areas covered by the scope can be effectively controlled by the management system.

Certification audits are always external audits. They are conducted by qualified auditors on behalf of a certification authority. External auditors generally operate based on the standards 'ISO/IEC 27006:2011 Requirements for bodies providing audit and certification of information security management systems' and 'ISO/IEC TS 17021-2:2012 Conformity assessment — Requirements for bodies providing audit and certification of management systems.'

Distinction between internal ISMS audits and the internal control system (ICS)

A company's internal control system (ICS) is an important control and monitoring instrument. Aspects of the ISMS can be a component of the internal control system, but the ICS generally goes far beyond the ISMS and primarily comprises specialized process controls.

In an ICS, a distinction is drawn between process-integrated and process-independent control activities. The former are usually control measures that result from the risk analysis, good management practices, or internal and external regulations (e.g., two-man rule for payment release, multi-factor authentication for critical users, etc.) and consequently could be based on the recommendations in ISO/IEC 2700x. This is what's known as the 'first line of defense;' it is intended to ensure the regularity of processes and activities in a company and is monitored directly by management.

Furthermore, an ISMS outside of IT/compliance can conduct a process-independent audit of the effectiveness of the control measures. This is often referred to as the 'second line of defense.' This audit does not replace internal auditing, which, as the 'third line of defense,' is intended to verify the effectiveness of the entire ICS.

- If an ICS is already in place, being set up, or being altered, it is recommendable to determine whether and to what extent the ISMS control and audit requirements have been taken into account and/or already partially integrated into the ICS. Complete integration is not possible in practice, as the objectives of the two systems are fundamentally different. However, organizational interfaces to the ICS and internal audit are always recommendable.
- COSO or COBIT can be used for modeling an ICS.

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- documentation of the audit program(s) (Clause 9.2 g)
- documentation of audit results (Clause 9.2 g)

References

ISO/IEC 27001:2013 – Clause 9.2
ISO/IEC 19011:2011
ISO/IEC 27007:2011
ISO/IEC 27006:2011
ISO/IEC TS 17021-2:2012

3.13 Incident Management

Although not explicitly mentioned in the normative section of the standard, the management of information security incidents is another essential component of a functional ISMS.

Incidents relevant to security are generally non-conformities that can have a decisive impact on the continuous improvement process (CIP) and the maturity of the ISMS if their causes are investigated. Ultimately, only when we recognize mistakes and learn from them, i.e. by rethinking our activities and strategies and removing or replacing ineffective measures, updating existing (security) concepts or implementing new (security) solutions, will we gain the greatest benefit from a management system operating in 'unpredictable' conditions (= risks) over the long term.

Success factors for practical implementation

In order to maintain information security in the course of normal operations, it is vital to anticipate ways for dealing with information security incidents to the greatest extent possible – e.g., by defining responsibilities, processes, and treatment options and rehearsing scenarios in advance.

The fundamental objective of the process for handling information security incidents is to ensure broadly coordinated, targeted, and efficient action if a security violation or targeted cyber-attack occurs.

- this chapter 'only' addresses the issue of 'information security incidents.' When developing a comprehensive contingency management system, please refer to ISO 22301:2012 'Societal security — Business continuity management systems — Requirements.'
- the organization must develop a logical way of categorizing incidents that clearly and practically distinguishes between varying degrees of severity – e.g., by differentiating between disruptions, security incidents, contingencies, and crises.

- a corresponding incident response plan must be drawn up that lays out the fundamental processes (see ISO/IEC 27002:2013). Naturally, it cannot cover every eventuality; if an incident occurs, it serves as a guideline and helps ensure that a targeted approach is taken.
- if a contingency occurs, the only procedures that will work are the ones that have been communicated and practiced multiple times in advance. If you count on the affected employees (who are they?) to know which section of the incident response plan to refer to (where did we put that again?) in order to immediately follow the pre-defined instructions in a worst-case scenario; if you assume that the managers in charge according to the plan will know what to do with the information that comes flooding in; then you won't be much better prepared when an a security incident occurs than someone without a plan – at least for the first few minutes or hours. But it is exactly this period of time that is crucial in a worst-case scenario.
- the process for responding to a security incident and the degree of detail in the plan should be in line with the organization's attitude toward risk and the framework of the ISMS.

Planning and Preparation

To achieve the fundamental objective of the process, preventative measures must be drawn up for all operational phases of the process in order to properly prepare the organization and its employees for a worst-case scenario. In addition to general problem-solving strategies, it is important to define contact persons and escalation paths in advance.

Identifying and Adopting

- regardless of their source, security incidents should always be reported to a central reporting authority. All relevant groups that could experience an IS incident (employees, IT suppliers, customers, partners, etc.) should be given clear reporting channels.
- rules for conduct if security-related irregularities occur, including points of contact/reporting plans, should be provided in a targeted way.

Classifying and Deciding

- the reporting authority decides if the incident reported is, in fact, a security incident, or if it is an incident unrelated to security, possibly referred to as a 'known error' for which a solution already exists, or if it is a contingency for which there is an contingency plan in place. When in doubt, escalation (possibly via a manager on duty) is the best course of action. The reporting authority must be properly trained.

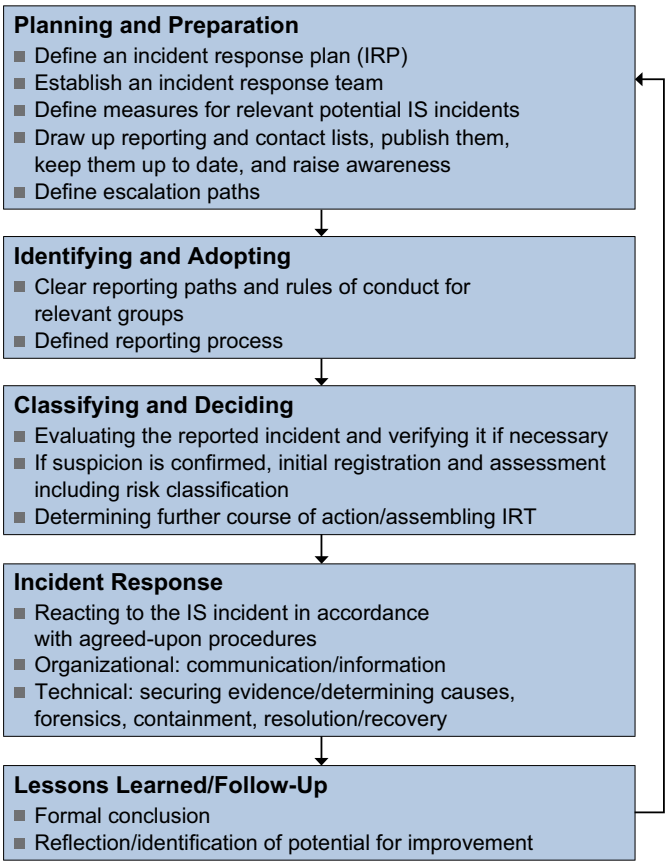


Figure 10: Incident response management – Phase model based on ISO/IEC 27035

- all incoming incident reports must be documented. At minimum, they should include the following information:
  - Clear identification number
  - Date of submission and occurrence of the security incident
  - Name(s) of the person/people making the report, name(s) of the person/people and information/IT systems affected
  - Description of the security incident (what approach did the attacker take, which vulnerabilities were exploited? Damage that has occurred thus far)
- all security incidents must be (initially) classified according to a previously approved classification scheme so that priorities can be determined. Depending on the respective priority, pre-defined measures for immediate action may need to be implemented and the responsible individuals (ISO, CISO, etc.) informed.
- the security incidents documented in the (ticket) system may need to be subjected to monitoring to ensure that incidents with a lower priority classification are also addressed.

Incident Response

In practice, the following approach has proven effective for incident response:

1. **containment and (initial) securing of evidence:** Analyzing the spread and containment of the security incident and (initially) securing potential evidence and proof by means of forensic analysis and methods that have been defined and tested (!) in advance (see Control A.16.1.7).

   Examples of local containment measures:
   - locking compromised user accounts
   - shutting down services that have been attacked/are at risk
   - using malware tools (virus scanners, anti-spyware or similar programs) to purge the system on the surface
   - examples within a network:
     - isolating compromised systems from the rest of the network and restricting access to a quarantine network
     - blocking specific services and/or protocols and certain IP addresses

2. **Resolution and recovery:** Measures to restore the desired configuration: In many cases, the system can be restored from a backup. Data and software are restored onto 'new' systems using 'clean' backup files; however, it must be ensured that all loopholes that may still be present in the backup are closed (install updates and patches if necessary) and that the backup files have not been altered in any way by an attacker.

   Another strategy is to update system software and harden the affected systems.

3. **Root cause analysis and (extended) securing of evidence:** Determining the root cause of the incident and securing potential evidence and proof, possibly by means of extended forensic analysis.

Lessons Learned/Follow-Up

- transparency is key any time a security incident occurs. This means that for every incident, the following must be clear:
  - The current processing status (new, accepted, in progress, halted, resolved, closed, etc.)
  - Which employees are responsible for handling the case
  - Which measures for resolving the problem are (currently) planned
  - When the required measures are scheduled to be implemented.
- after processing, all documented security incidents must be subjected to an audit to see if there is potential for improving the way similar incidents are handled in the future by optimizing the incident response plan or changing the structure and processes (e.g., creating/updating instructions for action).
- a report must always be drawn up when a security incident has been completely processed; it should indicate how similar incidents can be avoided in the future, or how their impact can be minimized. Further technical and organizational measures can be derived from this report; they must then be implemented in day-to-day operations.

Documentation requirements

According to ISO/IEC 27001:2013, no minimum documentation requirements apply.

Additionally, the following documents have proven useful in practice:

- incident response plan (IRP), including up-to-date (!) contact lists and escalation plans
- rules of conduct if security-related irregularities occur
- process descriptions and procedures for securing evidence
- IS incident reports

References

ISO/IEC 27001:2013 – A.16 (Annex A)
ISO/IEC 27035:2011
ISO 22301:2012

3.14 Continuous Improvement

No matter how many guidelines and books are written about 'optimal' management systems, it is unlikely that these systems will ever exist in practice; organizations are simply too different for a 'one-size-fits-all' solution. What's more, circumstances are constantly changing, so there can never be a permanent 'perfect solution.'

For this reason, organizations need to analyze existing best practices and always adapt them to their own needs. It is especially important that they take advantage of non-conformities to determine where there is room for improvement in their ISMS and constantly update their ISMS accordingly. This process is known as the continuous improvement process (CIP).

Consequently, an organization that wants to operate a standard-compliant ISMS must define organizational measures that form the basis for implementing the CIP in a targeted, scheduled way. The implementation of these measures and the subsequent results must be monitored and appropriately documented. The organization must also prove that it has implemented measures to ensure that any flaws detected will not reoccur.

PDCA (Plan-Do-Check-Act) cycle

The recommended approach for ensuring continuous improvement of the ISMS over the long term is still the PDCA cycle, which forms the foundation of numerous management systems.

- **Plan**
  - Establishing the control objectives and defining who is responsible for ensuring they are achieved
  - Establishing security measures for achieving the control objectives and defining the individuals responsible for the operational processes behind these measures
  - Defining performance indicators that allow performance to be measured against the control objectives
  - Defining the process for measuring performance, including the measurement points, methods for calculating the indicator, and the normal and tolerance ranges
  - Defining corrective actions to keep a security measure within the normal range
- **Do**
  - Continuous measurement of the achievement of objectives, delivered to security controlling within the ISMS
  - Implementation of corrective actions if flaws or non-conformities are identified
- **Check**
  - Monitoring individual security measure indicators and comparing individual performance with the control objectives
  - Supervising the implemented countermeasures and the individuals responsible for them if a security measure exceeds the normal effective range.
  - Drawing up security reports with key performance indicators for management based on the control objectives and security objectives. These reports should include recommendations for action for the required management decisions; they should strengthen security measures that exceed the normal range but are still within tolerance or that exceed threshold values and become ineffective.
- **Act**
  - Making the management decisions required to restore the effectiveness of security measures or entire objectives of measures. Decisions are handed down to day-to-day operations for implementation.
  - The decisions made are appropriately documented (e.g., via security controlling), including explanations.

Success factors for practical implementation

Improving the ISMS generally involves identifying deviations from the requirements and implementing the corrective actions defined as a result. However, it is also possible to immediately assess and implement suggestions for improvement without any existing deviations from the requirements.

Potential sources of deviations and suggestions for improvement

- conclusions from KPIs – analyses and measurements
- lessons learned from security incidents
- results of (internal) audits
- evaluation by management (management assessment)
- company suggestion program (suggestions for improvement)
- risk analyses carried out on a regular basis

- measures from the CIP should be integrated into the overarching implementation/risk treatment plan (which generally stems from the information security risk assessment) to create a centrally consolidated (or at least division-wide) list of measures.
- the risk analyses that must be conducted regularly also help to continuously improve the ISMS. The results of the risk analyses are a primary factor in improving the ISMS, as measures for minimizing risk are identified and included in risk treatment plans for implementation. Additionally, the risk treatment process involves monitoring these measures and evaluating their effectiveness.
- correction vs. corrective action: When an organization identifies flaws and non-conformities, it must react and correct/resolve them (see Clause 10.1 a) and b). Corrections resolve/rectify non-compliant situations. To prevent the same issue from occurring again, it is necessary to conduct a long-term root cause analysis and define corrective actions (see Clause 10.1 c to g).

Documentation requirements

The following minimum documentation requirements apply according to ISO/IEC 27001:2013:

- evidence of the type of non-conformities and all measures implemented in response (Clause 10.1 f)
- proof of the results of all corrective actions (Clause 10.1 g)

Additionally, the following documents have proven useful in practice:

- Procedures for corrective actions (from Clause 10.1 c onward)
- description of incident management and pursuit of corrective action
- documentation tool for tracking the status of implementation

References

ISO/IEC 27001:2013 – Clause 10
ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2015 – Annex SL

4. Glossary

ADV 'Auftragsdatenverarbeitung' (order data processing) – the processing of personal data by service providers (external, or internal by legally independent units of the corporation) in accordance with Section 11 of the German Federal Data Protection Act (BDSG).

APT Advanced persistent threat

Asset Anything that has value for the organization; also known as an information commodity or information asset. There are many types of assets, including: information, software, hardware, services, people and their qualifications, expertise and experience, and intangible assets such as reputation and image.

ISO/IEC 27005:2011 differentiates between primary and secondary assets; primary assets comprise business processes and business activities. Secondary assets support the primary assets: institutions, rooms, hardware, software, networks, personnel, and websites.

BDSG 'Bundesdatenschutzgesetz' (German Federal Data Protection Act)

BIA Business Impact Analysis

BSI 'Bundesamt für Sicherheit in der Informationstechnik' (German Federal Office for Information Security)

BSIMM Building Security in Maturity Model

CERT Computer Emergency Response Team

CIO Chief Information Officer

CIP Continuous improvement process

CIS Center for Internet Security

CISO Chief Information Security Officer

COBIT Control Objectives for Information and Related Technology – An internationally recognized framework for IT governance focusing on IT processes and control objectives.

COSO Committee of Sponsoring Organizations of the Treadway Commission – an American organization that developed the recognized standard for internal controls known as the COSO model.

DPO Data protection officer

EEA European Economic Area

EU European Union

ICS Internal control system

IEC International Electrotechnical Commission – An international standards body that cooperated with ISO to develop the standard ISO/IEC 2700x.

IS Information security

ISAE International Standard on Assurance Engagements

ISMS Information security management system – Part of the overarching management system based on business risk approach for establishing, implementing, operating, monitoring, maintaining, and improving information security.

The management system includes the organizational structure, policies, planning activities, responsibilities, practices, processes, and resources.

ISO International Organization for Standardization, publisher of international standards, including the ISO/IEC 2700x family.

ISO Information security officer

KPI Key performance indicator

MaRisk 'Mindestanforderungen an das Risikomanagement' (minimum requirements for risk management – administrative instructions for designing risk management programs at German credit institutions published by the German Federal Financial Supervisory Authority (BaFin).

QA Quality assurance

QAR-IT ISACA guideline for carrying out a quality assurance review of internal IT audits (QAR IT).

PDCA Plan-Do-Check-Act cycle – a continuous improvement process

RACI matrix Organizations use RACI categorizations to describe which roles are responsible for which activities and which roles must participate. This ensures that responsibilities and competencies are clearly described. The terms that comprise the acronym are defined as follows:

Responsible – In charge of actual execution *(implementation authority)*. The person who takes the initiative to assign responsibility for execution to others is also considered responsible in a disciplinary and qualitative sense.

Accountable – Answerable (*overall responsibility*), responsible in the sense of 'approve,' 'endorse,' or 'sign off on.' The person who assumes legal or commercial responsibility is also considered responsible from a cost center perspective.

Consulted – *(professional expertise)*. A person whose advice should or must be sought. Is also considered responsible from a professional perspective.

To be informed – *(right to information)*. A person who receives information about the progress/result of the task or is authorized to receive such information.

Generally, only one person (role) should be *accountable* for each activity. However, multiple people can be *responsible*, *consulted*, or *informed* for a given activity. Additionally, a single person can be both *accountable* and *responsible* for a given activity.

Risk Impact of uncertainty on objectives (definition according to ISO 31000:2009)

Scope Area of validity

SIRP Security Incident Response Process

SLA Service level agreement – Agreement between client and service provider

SMART Specific, measurable, attainable, realistic, timely

SoA Statement of applicability – Documented explanation of the relevant and applicable control objectives and measures in the organization's ISMS.

SoD matrix Segregation of duties matrix – Overview of the separation of functions among various roles within the organization that need to be considered.

TMG 'Telemediengesetz' (German Telemedia Act)

TOMs Technical and organizational measures

UWG 'Gesetz gegen den unlauteren Wettbewerb' (German Act against Unfair Competition)

Zero day vulnerability a vulnerability that has not been previously disclosed or corrected and that could be exploited to manipulate or attack computer applications, data, or other network services.

5. References

Norms and Standards

ISO 9001:2015 Quality management systems — Requirements
ISO 19011:2011 Guidelines for auditing management systems

ISO 22301:2012 Societal security — Business continuity management systems — Requirements

ISO 31000:2009 Risk management — Principles and guidelines

IEC 31010:2009 Risk management — Risk assessment techniques

ISO Guide 73:2009 Risk management — Vocabulary

ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls

ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance

ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement

ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management

ISO/IEC 27006:2011 Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2011 Information technology — Security techniques — Guidelines for information security management systems auditing

ISO/IEC 27018:2014 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cyber security

ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management

ISO/IEC 27036-1:2014 Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts

ISO/IEC 27036-2:2014 Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements

ISO/IEC 27036-3:2014 Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security

ISO/IEC Directives, Part 1, Consolidated ISO Supplement — Procedures specific to ISO, 2015

ISO/IEC FDIS 27017 Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC TR 27023:2015 Information technology – Security techniques – Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002

ISO/IEC TS 17021-2:2012 Conformity assessment — Requirements for bodies providing audit and certification of management systems

ONR 49000:2008 Risikomanagement für Organisationen und Systeme

Further Sources

COBIT 5 for Information Security, ISACA, 2012

BSI Standard 100-2 – IT-Grundschutz-Vorgehensweise (IT Baseline Protection Approach), Version 2.0, 2008

BSI Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz (Risk Analysis Based on IT Baseline Protection), Version 2.5, 2008

IT-Grundschutz-Kataloge des BSI (BSI IT Baseline Protection Catalogs), 14th Supplement, 2014

Guide – Cyber Security Check, BSI/ISACA Germany Chapter, 2014

SC27 Platinum Book – Twenty Years of ISO/IEC JTC1/SC27

Web Links

www.bsi.bund.de

www.enisa.europa.eu

www.esma.europa.eu

www.isaca.de

www.isaca.org

www.iso27001security.com

www.iso.org

www.jtc1sc27.din.de

6. Index of Figures

7. Appendix 1: Mapping ISO/IEC 27001:2013 vs. ISO/IEC 27001:2005

Key: ● = Complete coverage of contents ○ = Partial coverage of contents

ISO/IEC 27001:2013	Clauses in the standard (4 – 6)	ISO/IEC 27001:2005															
		4 Information security management system	4.1 General requirements	4.2 Establishing and managing the ISMS	4.2.1 Establish the ISMS	4.2.2 Implement and operate the ISMS	4.2.3 Monitor and review the ISMS	4.2.4 Maintain and improve the ISMS	4.3 Documentation requirements	4.3.1 General	4.3.2 Control of documents	4.3.3 Control of records	5 Management responsibility	5.1 Management commitment	5.2 Resource management	5.2.1 Provision of resources	5.2.2 Training, awareness and competence
4 Context of the organization																	
4.1 Understanding the organization and its context																	
4.2 Understanding the needs and expectations of interested parties																○	
4.3 Determining the scope of the information security management system				●					○								
4.4 Information security management system			●													○	
5 Leadership																	
5.1 Leadership and commitment					○									●			
5.2 Policy					●					○	○			●			
5.3 Organizational roles, responsibilities and authorities												○		●			
6 Planning																	
6.1 Actions to address risks and opportunities																	
6.1.1 General					●					○							
6.1.2 Information security risk assessment					●		○			○				○			
6.1.3 Information security risk treatment					●	○				○							
6.2 Information security objectives and planning to achieve them							○			○				●			
8.3 Preventive action																	
8.2 Corrective action																○	
8.1 Continual improvement																	
8 ISMS improvement																	
7.3 Review output																	
7.2 Review input																○	
7.1 General																	
7 Management review of the ISMS																	
6 Internal ISMS audits													○				
5.2.2 Training, awareness and competence																	
5.2.1 Provision of resources															○		
5.2 Resource management																	
5.1 Management commitment										○				●			
5 Management responsibility																	
4.3.3 Control of records													○				
4.3.2 Control of documents											○		○				
4.3.1 General					○					○							
4.3 Documentation requirements																	
4.2.4 Maintain and improve the ISMS																	
4.2.3 Monitor and review the ISMS																	
4.2.2 Implement and operate the ISMS																	
4.2.1 Establish the ISMS					●				○	●							
4.2 Establishing and managing the ISMS																	
4.1 General requirements				●													

ISO/IEC 27001:2013	ISO/IEC 27001:2005
Clauses in the standard (7 – 10)	**4 Information security management system**
	4.1 General requirements
	4.2 Establishing and managing the ISMS
	4.2.1 Establish the ISMS
7 Support	4.2.2 Implement and operate the ISMS ○
7.1 Resources	4.2.3 Monitor and review the ISMS
7.2 Competence	4.2.4 Maintain and improve the ISMS ○
7.3 Awareness	4.3 Documentation requirements
7.4 Communication	4.3.1 General ● ○
7.5 Documented information	4.3.2 Control of documents ● ●
7.5.1 General	4.3.3 Control of records ○ ●
7.5.2 Creating and updating	**5 Management responsibility**
7.5.3 Control of documented information	5.1 Management commitment ○
8 Operation	5.2 Resource management
8.1 Operational planning and control	5.2.1 Provision of resources ● ○
8.2 Information security risk assessment	5.2.2 Training, awareness and competence ● ●
8.3 Information security risk treatment	**6 Internal ISMS audits** ○ ●
9 Performance evaluation	**7 Management review of the ISMS**
9.1 Monitoring, measurement, analysis and evaluation	7.1 General ●
9.2 Internal audit	7.2 Review input ●
9.3 Management review	7.3 Review output ●
10 Improvement	**8 ISMS improvement**
10.1 Nonconformity and corrective action	8.1 Continual improvement ●
10.2 Continual improvement	8.2 Corrective action ●
	8.3 Preventive action ○ ●

ISO/IEC 27001:2013	ISO/IEC 27001:2005
Annex A (A.5 – A.9)	A.10.10 Monitoring
	A.10.9 Electronic commerce services
	A.10.8 Exchange of information
	A.10.7 Media handling
	A.10.6 Network security management
	A.10.5 Back-up
	A.10.4 Protection against malicious and mobile code
	A.10.3 System planning and acceptance
	A.10.2 Third party service delivery management
	A.10.1 Operational procedures and responsibilities
	A.10 Communications and operations management
	A.9.2 Equipment security
	A.9.1 Secure areas
	A.9 Physical and environmental security
	A.8.3 Termination or change of employment
	A.8.2 During employment
	A.8.1 Prior to employment
	A.8 Human resources security
	A.7.2 Information classification
	A.7.1 Responsibility for assets
	A.7 Asset management
	A.6.2 External parties
	A.6.1 Internal organization
	A.6 Organization of information security
	A.5.1 Information security policy
	A.5 Security policy

ISO/IEC 27001:2013	A.5	A.6	A.7	A.8	A.9	A.10	A.9.2	A.9.1	A.8.3	A.8.2	A.8.1	A.7.2	A.7.1	A.6.2	A.6.1	A.5.1
A.5 Information security policies																
A.5.1 Management direction for information security																●
A.6 Organisation of information security																
A.6.1 Internal organisation															○	
A.6.2 Mobile devices and teleworking																
A.7 Human resource security																
A.7.1 Prior to employment													●		○	
A.7.2 During employment												●				
A.7.3 Termination and change of employment									●							
A.8 Asset management																
A.8.1 Responsibility of assets									○		●					
A.8.2 Information classification												●				
A.8.3 Media handling										○						
A.9 Access control										●						
A.9.1 Business requirements for access control																
A.9.2 User access management									○							
A.9.3 User responsibilities																

ISO/IEC 27001:2013	ISO/IEC 27001:2005																	
Annex A (A.10 – A.13)	A.10.10 Monitoring											●						
	A.10.9 Electronic commerce services																	
	A.10.8 Exchange of information																	●
	A.10.7 Media handling																	
	A.10.6 Network security management																●	
	A.10.5 Back-up										●							
	A.10.4 Protection against malicious and mobile code									●								
	A.10.3 System planning and acceptance								○									
	A.10.2 Third party service delivery management																	
	A.10.1 Operational procedures and responsibilities								●									
	A.10 Communications and operations management																	
	A.9.2 Equipment security						●											
	A.9.1 Secure areas					●												
	A.9 Physical and environmental security																	
	A.8.3 Termination or change of employment																	
	A.8.2 During employment																	
	A.8.1 Prior to employment																	
	A.8 Human resources security																	
	A.7.2 Information classification																	
	A.7.1 Responsibility for assets																	
	A.7 Asset management																	
	A.6.2 External parties																	
	A.6.1 Internal organization																	○
	A.6 Organization of information security																	
	A.5.1 Information security policy																	
	A.5 Security policy																	
	A.9.4 System and application access control		**A.10 Cryptography**	A.10.1 Cryptographic controls	**A.11 Physical and environmental security**	A.11.1 Secure areas	A.11.2 Equipment	**A.12 Operations security**	A.12.1 Operational procedures and responsibilities	A.12.2 Protection from malware	A.12.3 Backup	A.12.4 Logging and monitoring	A.12.5 Control of operational software	A.12.6 Technical vulnerability management	A.12.7 Information systems audit considerations	**A.13 Communications strategy**	A.13.1 Network security management	A.13.2 Information transfer

ISO/IEC 27001:2013	ISO/IEC 27001:2005																
Annex A (A.14 – A.18)	A.10.10 Monitoring																
	A.10.9 Electronic commerce services																
	A.10.8 Exchange of information																
	A.10.7 Media handling																
	A.10.6 Network security management																
	A.10.5 Back-up																
	A.10.4 Protection against malicious and mobile code																
	A.10.3 System planning and acceptance			○				○						○			
	A.10.2 Third party service delivery management						●	●									
	A.10.1 Operational procedures and responsibilities																
	A.10 Communications and operations management																
	A.9.2 Equipment security																
	A.9.1 Secure areas																
	A.9 Physical and environmental security																
	A.8.3 Termination or change of employment																
	A.8.2 During employment																
	A.8.1 Prior to employment																
	A.8 Human resources security																
	A.7.2 Information classification																
	A.7.1 Responsibility for assets																
	A.7 Asset management																
	A.6.2 External parties						●										
	A.6.1 Internal organization																○
	A.6 Organization of information security																
	A.5.1 Information security policy																
	A.5 Security policy																
	A.14 System acquisition, development and maintenance																
	A.14.1 Security requirements for Information systems																
	A.14.2 Security in development and support processes																
	A.14.3 Test data																
	A.15 Supplier relationships																
	A.15.1 Information security in supplier relationships																
	A.15.2 Supplier service delivery management																
	A.16 Information security incident management																
	A.16.1 Management of information security incidents and management																
	A.17 Information security aspects of business continuity management																
	A.17.1 Information security continuity																
	A.17.2 Redundancies																
	A.18 Compliance																
	A.18.1 Compliance with legal requirements																
	A.18.2 Information security reviews																

ISO/IEC 27001:2013	ISO/IEC 27001:2005									
Annex A (A.5 – A.7) cont.	A.15.3 Information systems audit considerations									
	A.15.2 Compliance with security policies and standards, and technical compliance									
	A.15.1 Compliance with legal requirements									
	A.15 Compliance									
	A.14.1 Information security aspects of business continuity management									
	A.14 Business continuity management									
	A.13.2 Management of information security incidents and improvements									
	A.13.1 Reporting information security events and weaknesses									
	A.13 Information security incident management									
	A.12.6 Technical vulnerability management									
	A.12.5 Security in development and support processes									
	A.12.4 Security of system files									
	A.12.3 Cryptographic controls									
	A.12.2 Correct processing in applications									
	A.12.1 Security requirements of information systems									
	A.12 Information systems acquisition, development and maintenance									
	A.11.7 Mobile computing and teleworking					●				
	A.11.6 Application and information access control									
	A.11.5 Operating system access control									
	A.11.4 Network access control									
	A.11.3 User responsibilities									
	A.11.2 User access management									
	A.11.1 Business requirement for access control									
	A.11 Access control									
	A.5 Information security policies									
	A.5.1 Management direction for information security									
	A.6 Organisation of information security									
	A.6.1 Internal organisation									
	A.6.2 Mobile devices and teleworking									
	A.7 Human resource security									
	A.7.1 Prior to employment									
	A.7.2 During employment									
	A.7.3 Termination and change of employment									

Annex A (A.8 – A.9) cont.

ISO/IEC 27001:2013	ISO/IEC 27001:2005									
A.8 Asset management	A.15.3 Information systems audit considerations									
A.8.1 Responsibility of assets	A.15.2 Compliance with security policies and standards, and technical compliance									
A.8.2 Information classification	A.15.1 Compliance with legal requirements									
A.8.3 Media handling	**A.15 Compliance**									
A.9 Access control	A.14.1 Information security aspects of business continuity management									
A.9.1 Business requirements for access control	**A.14 Business continuity management**									
A.9.2 User access management	A.13.2 Management of information security incidents and improvements									
A.9.3 User responsibilities	A.13.1 Reporting information security events and weaknesses									
A.9.4 System and application access control	**A.13 Information security incident management**									
	A.12.6 Technical vulnerability management									
	A.12.5 Security in development and support processes				○					
	A.12.4 Security of system files									○
	A.12.3 Cryptographic controls									
	A.12.2 Correct processing in applications									
	A.12.1 Security requirements of information systems									
	A.12 Information systems acquisition, development and maintenance									
	A.11.7 Mobile computing and teleworking									
	A.11.6 Application and information access control									●
	A.11.5 Operating system access control									●
	A.11.4 Network access control						○			
	A.11.3 User responsibilities								●	
	A.11.2 User access management							●		
	A.11.1 Business requirement for access control						●			
	A.11 Access control									

ISO/IEC 27001:2013	ISO/IEC 27001:2005									
Annex A (A.10 – A.12) cont.	A.15.3 Information systems audit considerations									
	A.15.2 Compliance with security policies and standards, and technical compliance									
	A.15.1 Compliance with legal requirements									
	A.15 Compliance									
	A.14.1 Information security aspects of business continuity management									
	A.14 Business continuity management									
	A.13.2 Management of information security incidents and improvements									
	A.13.1 Reporting information security events and weaknesses									
	A.13 Information security incident management									
	A.12.6 Technical vulnerability management									
	A.12.5 Security in development and support processes					○				
	A.12.4 Security of system files									
	A.12.3 Cryptographic controls		●							
	A.12.2 Correct processing in applications									
	A.12.1 Security requirements of information systems									
	A.12 Information systems acquisition, development and maintenance									
	A.11.7 Mobile computing and teleworking									
	A.11.6 Application and information access control									
	A.11.5 Operating system access control									
	A.11.4 Network access control									
	A.11.3 User responsibilities					○				
	A.11.2 User access management									
	A.11.1 Business requirement for access control									
	A.11 Access control									
	A.10 Cryptography									
	A.10.1 Cryptographic controls									
	A.11 Physical and environmental security									
	A.11.1 Secure areas									
	A.11.2 Equipment									
	A.12 Operations security									
	A.12.1 Operational procedures and responsibilities									
	A.12.2 Protection from malware									
	A.12.3 Backup									

ISO/IEC 27001:2013	ISO/IEC 27001:2005							
	A.15.3 Information systems audit considerations				●			
	A.15.2 Compliance with security policies and standards, and technical compliance							
	A.15.1 Compliance with legal requirements							
	A.15 Compliance							
	A.14.1 Information security aspects of business continuity management							
	A.14 Business continuity management							
	A.13.2 Management of information security incidents and improvements							
	A.13.1 Reporting information security events and weaknesses							
	A.13 Information security incident management							
	A.12.6 Technical vulnerability management			●				
	A.12.5 Security in development and support processes			○				
	A.12.4 Security of system files		●	○				
	A.12.3 Cryptographic controls							
	A.12.2 Correct processing in applications							
	A.12.1 Security requirements of information systems							
	A.12 Information systems acquisition, development and maintenance							
	A.11.7 Mobile computing and teleworking							
	A.11.6 Application and information access control							
	A.11.5 Operating system access control							
	A.11.4 Network access control						○	
	A.11.3 User responsibilities							
	A.11.2 User access management							
	A.11.1 Business requirement for access control							
	A.11 Access control							
Annex A (A.12 – A.13) cont.	A.12.4 Logging and monitoring							
	A.12.5 Control of operational software							
	A.12.6 Technical vulnerability management							
	A.12.7 Information systems audit considerations							
	A.13 Communications strategy							
	A.13.1 Network security management							
	A.13.2 Information transfer							

ISO/IEC 27001:2013	ISO/IEC 27001:2005							
	A.15.3 Information systems audit considerations							
	A.15.2 Compliance with security policies and standards, and technical compliance							
	A.15.1 Compliance with legal requirements							
	A.15 Compliance							
	A.14.1 Information security aspects of business continuity management							
	A.14 Business continuity management							
	A.13.2 Management of information security incidents and improvements							
	A.13.1 Reporting information security events and weaknesses							
	A.13 Information security incident management							
	A.12.6 Technical vulnerability management							
	A.12.5 Security in development and support processes			●				
	A.12.4 Security of system files				●			
	A.12.3 Cryptographic controls							
	A.12.2 Correct processing in applications		○	○				
	A.12.1 Security requirements of information systems		●					
	A.12 Information systems acquisition, development and maintenance							
	A.11.7 Mobile computing and teleworking							
	A.11.6 Application and information access control							
	A.11.5 Operating system access control							
	A.11.4 Network access control							
	A.11.3 User responsibilities							
	A.11.2 User access management							
	A.11.1 Business requirement for access control							
	A.11 Access control							
Annex A (A.14 – A.15) cont.	**A.14 System acquisition, development and maintenance**							
	A.14.1 Security requirements for Information systems							
	A.14.2 Security in development and support processes							
	A.14.3 Test data							
	A.15 Supplier relationships							
	A.15.1 Information security in supplier relationships							
	A.15.2 Supplier service delivery management							

ISO/IEC 27001:2013	ISO/IEC 27001:2005								
Annex A (A.16 – A.18) cont.	A.15.3 Information systems audit considerations								
	A.15.2 Compliance with security policies and standards, and technical compliance								●
	A.15.1 Compliance with legal requirements							●	
	A.15 Compliance								
	A.14.1 Information security aspects of business continuity management				●				
	A.14 Business continuity management								
	A.13.2 Management of information security incidents and improvements		●						
	A.13.1 Reporting information security events and weaknesses		●						
	A.13 Information security incident management								
	A.12.6 Technical vulnerability management								
	A.12.5 Security in development and support processes								
	A.12.4 Security of system files								
	A.12.3 Cryptographic controls								
	A.12.2 Correct processing in applications								
	A.12.1 Security requirements of information systems								
	A.12 Information systems acquisition, development and maintenance								
	A.11.7 Mobile computing and teleworking								
	A.11.6 Application and information access control								
	A.11.5 Operating system access control								
	A.11.4 Network access control								
	A.11.3 User responsibilities								
	A.11.2 User access management								
	A.11.1 Business requirement for access control								
	A.11 Access control								
	A.16 Information security incident management								
	A.16.1 Management of information security incidents and management								
	A.17 Information security aspects of business continuity management								
	A.17.1 Information security continuity								
	A.17.2 Redundancies								
	A.18 Compliance								
	A.18.1 Compliance with legal requirements								
	A.18.2 Information security reviews								

8. Appendix 2: Version Comparison, ISO/IEC 27001:2013 vs. ISO/IEC 27001:2005

The following is a brief explanation of the most significant changes made to the content of ISO/IEC 27001:2013 compared to the previous version from 2005.

The biggest change in terms of **management** is the removal of measure A.6.1.1, '*Management commitment to information security*,' from 2005 and the increased integration of the requirements facing company management into the principles of information security management in Clause 5.1 of the 2013 version of the standard. Additionally, the term 'top management' is more frequently used instead of the term 'management' (see Clauses 5 and 9.3). This change places a much stronger focus on the fundamental importance of commitment among the highest level of management. Furthermore, the new version explicitly requires that the information security objectives be clearly consistent with the business objectives; top management is responsible for ensuring that this is the case.

The **integration of information security** into other business processes and into all projects in general is an explicit requirement in the latest version (see measure A.6.1.5 '*Information security in project management*').

The 2005 version required business, legal or governmental requirements and contractual security obligations to be described in the context of the **information security policy**. Under the 2013 version, this will likely be handled in the scope document (see Clause 4). Moreover, the information security policy no longer needs to define (all) criteria for risk management in the context of information security. They will now be included in correspondingly detailed methodology descriptions and/or in separately developed risk strategies on information security (see Clause 6.1).

The exceptional importance of **risk management** in the context of an ISMS is highlighted more prominently than ever in the 2013 version of the standard (see Clause 0.1). Additionally, the subject is structured more clearly than in the previous version. In the previous version, risk management requirements were spread out throughout a number of different clauses, such as the sub-items of Clause 4.2.1 '*Establish the ISMS*.' Now, three whole clauses are dedicated solely to this subject (see Clauses 6.1, 8.2, and 8.3).

The requirement of a risk treatment plan is still a central aspect (see Clause 8.3 of ISO/IEC 27001:2013 vs. Clauses 4.2.2 and 7.3 of ISO/IEC 27001:2005).

The requirements in terms of the **roles and responsibilities** necessary in the context of an ISMS are located in different clauses of ISO/IEC 27001:2013, but they essentially already existed in the 2005 version (see Clauses 5.3, 7.1, and 7.2 of ISO/IEC 27001:2013 vs. Clauses 5.2.1 and 5.2.2 of ISO/IEC 27001:2005).

In the 2005 version, the monitoring and measurement of the effectiveness of security measures were a sub-item of the clause '*Management Review*' (see Clauses 4.2.2 d and 4.2.3). It listed several general requirements in terms of monitoring and reviewing the ISMS. The guidelines from ISO/IEC 27004:2009 were not explicitly mentioned and, at most, could have been considered a recommendation. Greater attention is paid to the subject in the 2013 version; it even has its own dedicated clause. Documentation requirements for performance monitoring are now an obligatory element for potential certification (see Clause 9.1).

No fundamental changes were made to the requirements for **internal audits** (see Clause 9.2 of ISO/IEC 27001:2013 vs. Clauses 4.2.3 e and 6 of ISO/IEC 27001:2005). Internal audits still have to be conducted; however, process documentation describing the procedure does not need to be drawn up. However, for larger institutions, it is still recommendable to formally document this process so that multiple organizational units responsible for internal audits will use an identical process, and so that clear boundaries will be drawn between the responsibilities of these audit departments (ISMS audits, internal audit, data protection, technical IT security audits, etc.). The creation and implementation of a sufficiently detailed audit program, on the other hand, is explicitly required (see Clause 9.2 c). Clause 9.2 a, Sentence 2 could lead readers to assume that the requirements are now less restrictive than they were in Clause 6 of the 2005 version. This is not the case, however. Internal audits must take *all* requirements from the standard into account. In that sense, compliance with relevant legislation and regulations and the existing requirements of interest groups must also be considered (see Clause 4.2 and 4.3).

In terms of **documentation** requirements, an important difference between the 2005 and 2013 versions is that Clause 7.5 of the 2013 version no longer includes an explicit list

of the documents to be drawn up. The specific information and documents required are now exclusively based on the requirements in the individual clauses and, depending on the scope, the requirements laid out in Annex A.

The most important changes in the context of **communication** relate to the subject's inclusion in its own clause (see Clause 7.4) and the explicit requirements for internal and external communication. The requirements are now much more specific than they were in the previous version, but generally speaking, they are still in line with standard practices.

In the old standard, the subject of **awareness** was only explicitly addressed in a single sentence (see Clause 5.2.2). The new standard, on the other hand, has a whole clause dedicated to this subject, highlighting the importance of awareness campaigns. Three specific requirements are defined; evidence must be provided that they have been met (see Clause 7.3).

The 2013 version places clear emphasis on the topics of **outsourcing** and **supplier relationships** and even dedicates a control domain in Annex A to the latter subject (see A.15 '*Supplier relationships*'). Unlike the previous version, the standard no longer refers (solely) to *stakeholders* whose requirements and expectations must be initially determined; it uses the more far-reaching term *interested parties*. *Suppliers* are explicitly listed (see Chapter 3.1 *Context of the Organization* in this guideline). However, the standard is restrained when it comes to specific requirements for implementation, instead leaving this up to ISO/IEC 27036, for which certification is not available.

A significant change in terms of **continuous improvement** is that the plan-do-check-act cycle (PDCA) is no longer explicitly required. Instead, any form of organization that supports continuous improvement can be used. However, the structure and content of the standard (Clauses 4 to 10) results in a PDCA cycle which operates 'in the background:'

- Plan: Context/management functions/planning (Clauses 4, 5, and 6)
- Do: Framework/support/implementation (Clauses 7 and 8)
- Check: Monitoring (Clause 9)
- Act: Reaction/improvement (Clause 10)

The standard no longer specifically requires the implementation of **preventative measures**. However, this requirement is implicitly included in Clauses 6.1.1 and 10.1. Clause 10.1 requires that the repercussions of identified errors be dealt with. In practice, this means that not only the immediate repercussions, but also future repercussions and their risk potential must be considered. This is clearly highlighted once again in Clause 10.1 b, which requires the evaluation of measures for eliminating the *causes* of an error so that the error does not reoccur or occur somewhere else (treating the symptoms vs. treating the cause). This means that the cause(s) of the error must be investigated and preventative measures must be effectively implemented so that the error does not occur again.

In that sense, ISO/IEC 27001:2013 no longer treats preventative measures as a separate step; they are instead treated as a necessary requirement that is integrated into all steps of the process. Identifying and eliminating the causes of errors are intended to prevent the error from occurring again, which ultimately helps to improve the ISMS as a whole. ISO/IEC 27001:2013 does not use the term 'errors;' rather, it refers to non-conformities (distinction: ISO/IEC 27002:2013 still uses the term 'error,' however).

Summary

The 2013 version is not a fundamental reorientation of the standard. Efficient, appropriate risk management remains one of the key aspects of ISO/IEC 27001. The supporting processes are also still necessary. They are now described in more precise terms, and their synergy within the overall management system is highlighted more strongly than before. Overall, even with the updates to ISO/IEC 27002 that were made at the same time, the new version is a clear, robust standard that will continue to be a great help to managers tasked with setting up and operating an ISMS.

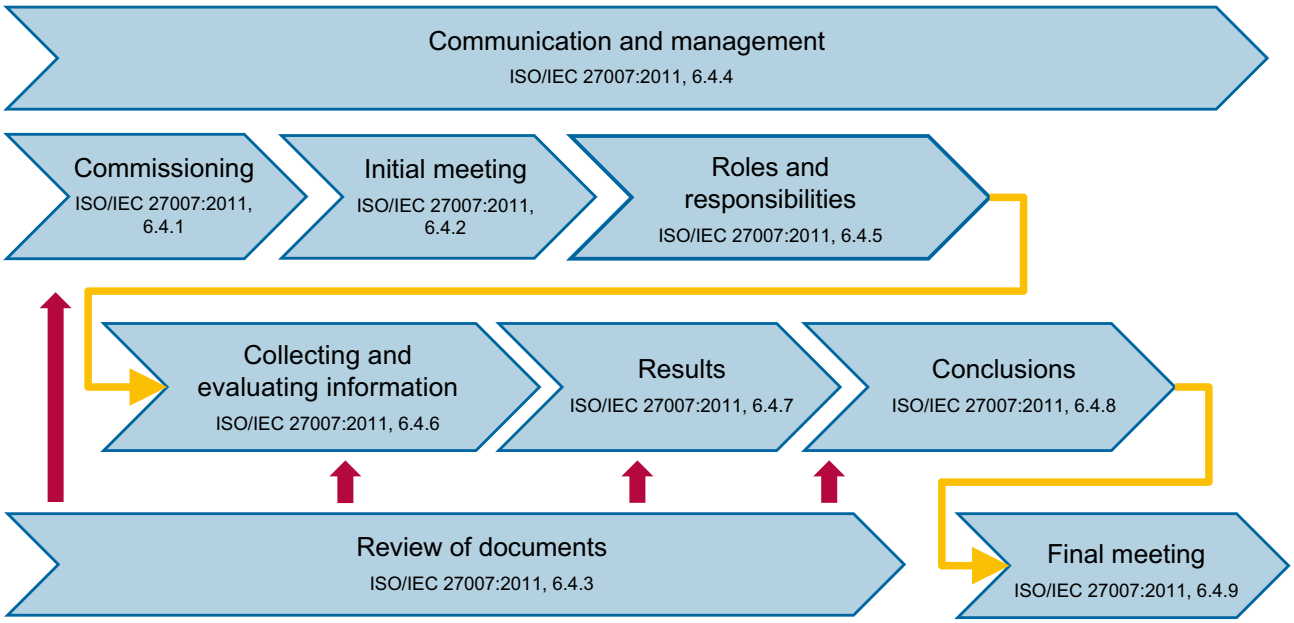
Other newly published management standards are also in line with the ISO/IEC directives (Annex SL), such as ISO 9001:2015 and ISO 22301:2012. This is intended to facilitate harmonization of the management systems and improve the way they work together. This simultaneously streamlines the process for acquiring certifications for multiple standards at the same time, allowing companies to meet recurring requirements for different management systems using one holistic approach and 'under one roof.'

9. Appendix 3: Internal ISMS Audits – Mapping of ISO/IEC 19011:2011 and ISO/IEC 27007:2011

Requirements for internal ISMS audits from ISO/IEC 27001:2013 vs. ISO/IEC 19011 & ISO/IEC 27007

Sub-process/Activity	ISO/IEC 27001:2013	ISO/IEC 19011:2011 ISO/IEC 27007:2011
Planning the audit program	9.2 a 9.2 b 9.2 c	5.1 General 5.2 Establishing the audit program objectives
Establishing the audit program	9.2 c	5.3 Establishing the audit program
Implementing the audit program	9.2 c	5.4 Implementing the audit program
Monitoring the audit program	9.2 c	5.5 Monitoring the audit program
Reviewing and improving the audit program	9.2 c	5.6 Reviewing and improving the audit program
Expertise and selection of auditors	9.2 e	7 Competence and evaluation of auditors
Documentation and evidence	9.2 g	5.4.7 Managing and maintaining audit program records
Defining the audit criteria and scope for each audit	9.2 d	5.4.2 Defining the objectives, scope and criteria for an individual audit
Performing ISMS audits	9.2 e	6 Performing an audit
Reporting audit results	9.2 f	5.4.6 Managing the audit program outcome

10. Appendix 4: Performing Internal ISMS Audits (Process Diagram)




CISA
Certified Information Systems Auditor
An ISACA Certification
CISM
Certified Information Security Manager
An ISACA Certification
CRISC
Certified in Risk and Information Systems Control
An ISACA Certification
CGEIT
Certified in the Governance of Enterprise IT
An ISACA Certification