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

Implementation Guide ISO/IEC 27001:2022

Practical guide for the implementation of an information security management system (ISMS) according to ISO/IEC 27001:2022

ISACA Germany Chapter

dpunkt.verlag

Publisher
ISACA Germany Chapter e. V.
Storkower Str. 158
10407 Berlin

www.isaca.de
info@isaca.de

Author team 2022

- Erik Gremeyer (CISA, CISM), ATM Consulting
- Andreas Kirchner (CISM, CISSP), abat AG
- Ralf Knecht (CISM)
- Ying-Yeung John Man (CISA, CISM)
- Dirk Meissner (CISA, CDPSE), Allevio AG
- Nico Müller (CISA, CISM, ITGM)
- Jan Rozek
- Dr. Markus Ruppel, RIMOC GmbH
- Andrea Rupprich (CISA, CISM), usd AG
- Dr. Tim Sattler (CISA, CISM, CGEIT, CRISC, CDPSE, CISSP, CCSP), Jungheinrich AG
- Michael Schmid (CISM), Hubert Burda Media

Team of authors 2016

- 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, CGEIT, CRISC, CISSP), Jungheinrich AG
- Michael Schmid (CISM), Hubert Burda Media
- Holger Schrader (CISM, CRISC)

Status: November 2022 (Final after review and revision by ISACA Information Security Specialist Group).

Machine translation

Implementation Guide ISO/IEC 27001:2022

Practical guide for the implementation of an information security management system (ISMS) according to ISO/IEC 27001:2022

ISACA
Germany Chapter

Why this guide?

Information security is indispensable. As a component of corporate management, it must be geared to providing optimum support for business objectives. Even or especially in times of so-called "cyber threats" and the emerging challenges of "cyber security" in many places, a well-structured information security management system (ISMS) in accordance with internationally recognized standards provides the optimal basis for the efficient and effective implementation of a holistic information security strategy.

Whether the chosen focus is on threats originating from the Internet, the protection of intellectual property, the fulfillment of regulations and contractual obligations, or the safeguarding of production systems depends on the framework conditions (e.g., industry, business model, or risk appetite) and the specific security objectives of the respective organization. In all cases, it is crucial to be aware of the existing information security risks in the respective context or to uncover them and to select, implement and ultimately also consistently track the necessary strategies, processes and security measures.

The concrete implementation of an ISMS requires experience, but is based first and foremost on the decision and commitment of top management to the subject. A clear management mandate and a security strategy adapted to the business strategy, together with competent personnel and the resources that are ultimately always required, are the basic prerequisites for optimally supporting the achievement of business objectives with an ISMS.

The updated *Implementation Guide ISO/IEC 27001: 2022* (in short: Implementation Guide) contains practical recommendations and advice for organizations that either already operate an ISMS in accordance with the international ISO/IEC standard 27001, "Information security, cybersecurity and privacy protection - Information security management sys- tems - Requirements", or wish to establish one, irrespective of existing or possible certification. The guide offers pragma- tic assistance and approaches to all those entrusted with the establishment and/or operation of an ISMS. The advantages of an individually adapted and, if necessary, simultaneously standard-compliant ISMS are clearly highlighted. In particular, practical recommendations for establishing or increasing the maturity level of existing ISMS processes and typical implementation examples of various requirements are presented.

Acknowledgement

ISACA Germany Chapter e.V. would like to thank the ISACA Information Security Group and the authors for preparing the guide: Erik Gremeyer, Andreas Kirchner, Ralf Knecht, Ying-Yeung John Man, Dirk Meissner, Nico Müller, Jan Rozek, Dr. Markus Ruppel, Andrea Rupprich, Dr. Tim Sattler, Michael Schmid.

Project management and editing: Andrea Rupprich

Table of contents

1 Introduction

The systematic management of information security in accordance with ISO/IEC 27001:2022 is intended to ensure effective protection of information and IT systems with regard to the essential protection goals of information security (confidentiality, integrity and availability).

This protection is not an end in itself, but serves to support business processes, achieve corporate goals and preserve corporate values through the trouble-free provision and processing of information. In practice, an ISMS uses the following three perspectives for this purpose:

- **G - Governance view**
  - IT goals and information security objectives derived from the
    are derived from higher-level corporate goals (e.g. supported by or derived from COSO or COBIT)
- **R - Risk view**
  - Protection needs and risk exposure of the corporate values and IT systems
  - Risk appetite of the company
  - Opportunities and risks
- **C - Compliance view**
  - External requirements due to laws, regulations and Standards
  - Internal specifications and guidelines
  - Contractual obligations

These views determine which protective measures are appropriate and effective for

- the organization's capabilities and business processes,
- the need for protection depending on the criticality of the respective company assets as well as
- compliance with applicable laws and regulations.

Measures

On the one hand, measures to achieve and maintain fault-free information processing must *be effective in order* to achieve the required level of protection. On the other hand, they must also be *economically appropriate (efficient)*.

ISO/IEC 27001:2022 and the requirements and measures systematically and comprehensively set out therein, which - in varying degrees and quality - are part of the operation of every ISMS, support the achievement of the objectives listed at the beginning from all three perspectives (see Fig. 1):

- The *governance view* refers to the control aspects of the ISMS, such as close involvement of the management.
  The following aspects must be taken into account: the commitment of top management (see section *3.2 Leadership and Commitment*), consistency between business and information security objectives (see section *3.3 IS Objectives),* the definition of strategies and guidelines (see section *3.4 IS Policy),* an effective communication strategy tailored to the target group (see section 3.9 Communication), appropriate responsibilities and organizational structures (see section 3.5 Roles, Responsibilities, and Competencies), and targeted monitoring of performance (see section 3.7 *IS Objectives).* Chapter *3.9 Communication*), appropriate responsibilities and organizational structures (see Chapter *3.5 Roles, Responsibilities, and Competencies*), and targeted performance monitoring (see Chapter *3.7 Performance/Risk/Compliance Monitoring*). ISO/IEC 27014:2020 provides further information on the governance of information security.
- The *risk view*, which serves among other things as a basis for comprehensible decision-making and prioritization of risks, is a key element of the *risk management process.*
  It is represented by IS risk management (cf. Section *3.6 Risk Management*) and includes specifications and methods for identifying, analyzing and assessing risks in the context of information security, i.e. risks that represent 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 view* is firmly anchored in the entire standard. On the one hand, it includes the definition of required
(security) requirements, which is supported by the measures from Annex A. On the other hand, it refers to the concrete fulfillment of precisely these requirements, which is supported by regular monitoring on the part of management and those responsible for information security (cf. Section *3.7 Performance/Risk/Compliance* monitoring) and by internal audits (cf. chapters *3.12 Internal Audit* and *3.14 Continual Improvement*). Appropriate documentation (see chapter *3.8 Documentation*) and the existing security awareness of employees and managers (see chapter *3.10 Awareness*) are also essential for the compliance view.

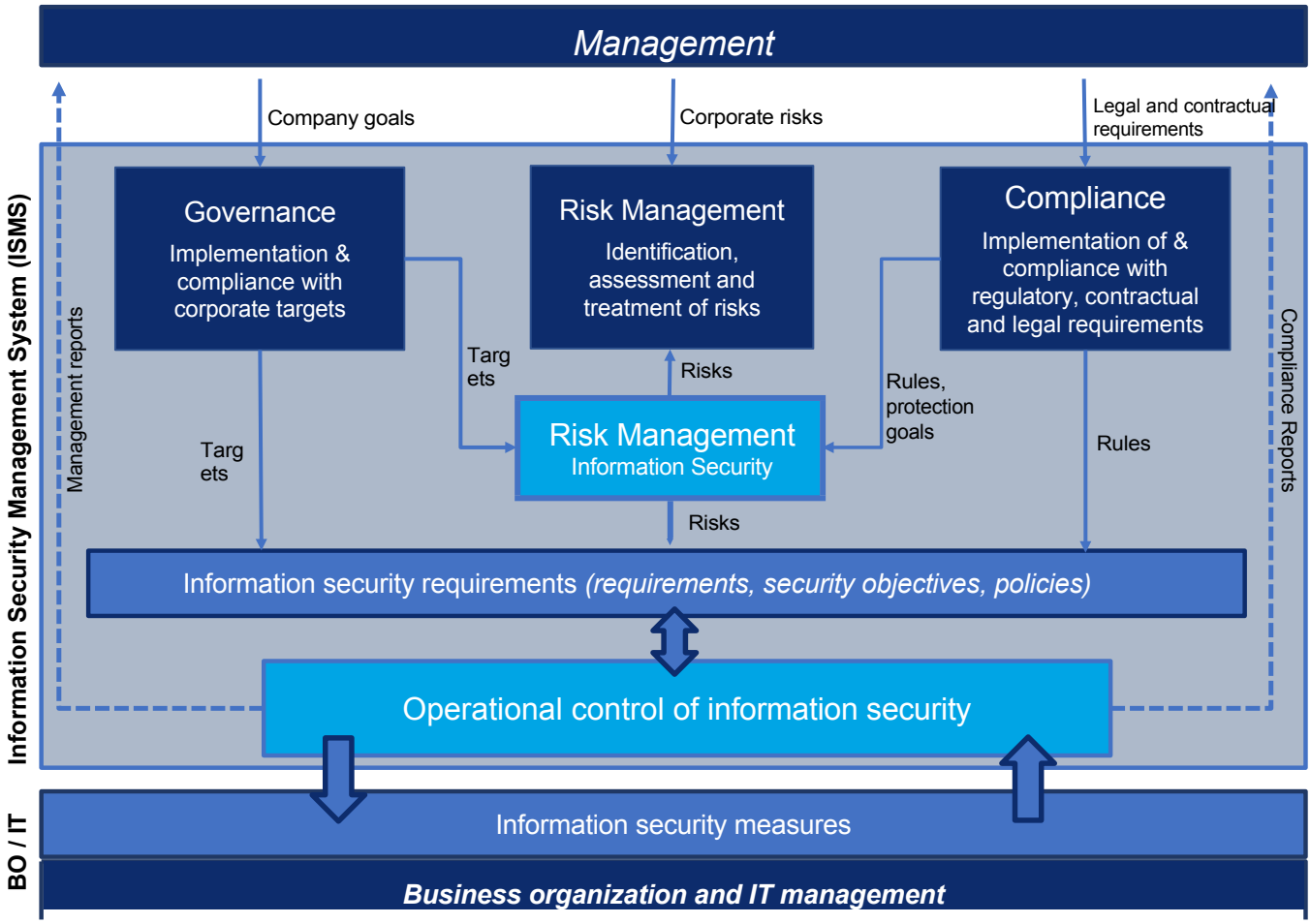


Figure 1: Integration of the ISMS into corporate [management1]

1Source : Carmao GmbH.

2 Structure of the guide

2.1 Topics

This implementation guide i s based on the main topics of the ISO/IEC 27001:2022 standard, but without reproducing the section structure of the standard identically. Instead, the relevant subject areas of an ISMS according to ISO/IEC 27001:2022 are described as "building blocks" that have proven to be relevant and necessary in practice. Against this background, the contents of the relevant sections of the standard are restructured and combined into individual focal topics. From the authors' point of view, the 14 "building blocks" listed below can be highlighted on the basis of the standard, which together represent the ISMS of an organization (see Figure 2):

1. Context of the Organization (Context of the Organization)
2. Leadership and Commit- ment (Leadership and Commit- ment)
3. IS Objectives
4. IS Policy (IS Policy)
5. Roles, Responsibilities, and Competencies
6. Risk Management
7. Evaluation of performance and KPIs (performance/risk/compliance monitoring)
8. Documentation (Documentation)
9. Communication
10. Awareness (Awareness)
11. Supplier Relationships
12. Internal Audit (Internal Audit)
13. Incident Management
14. Continuous Improvement

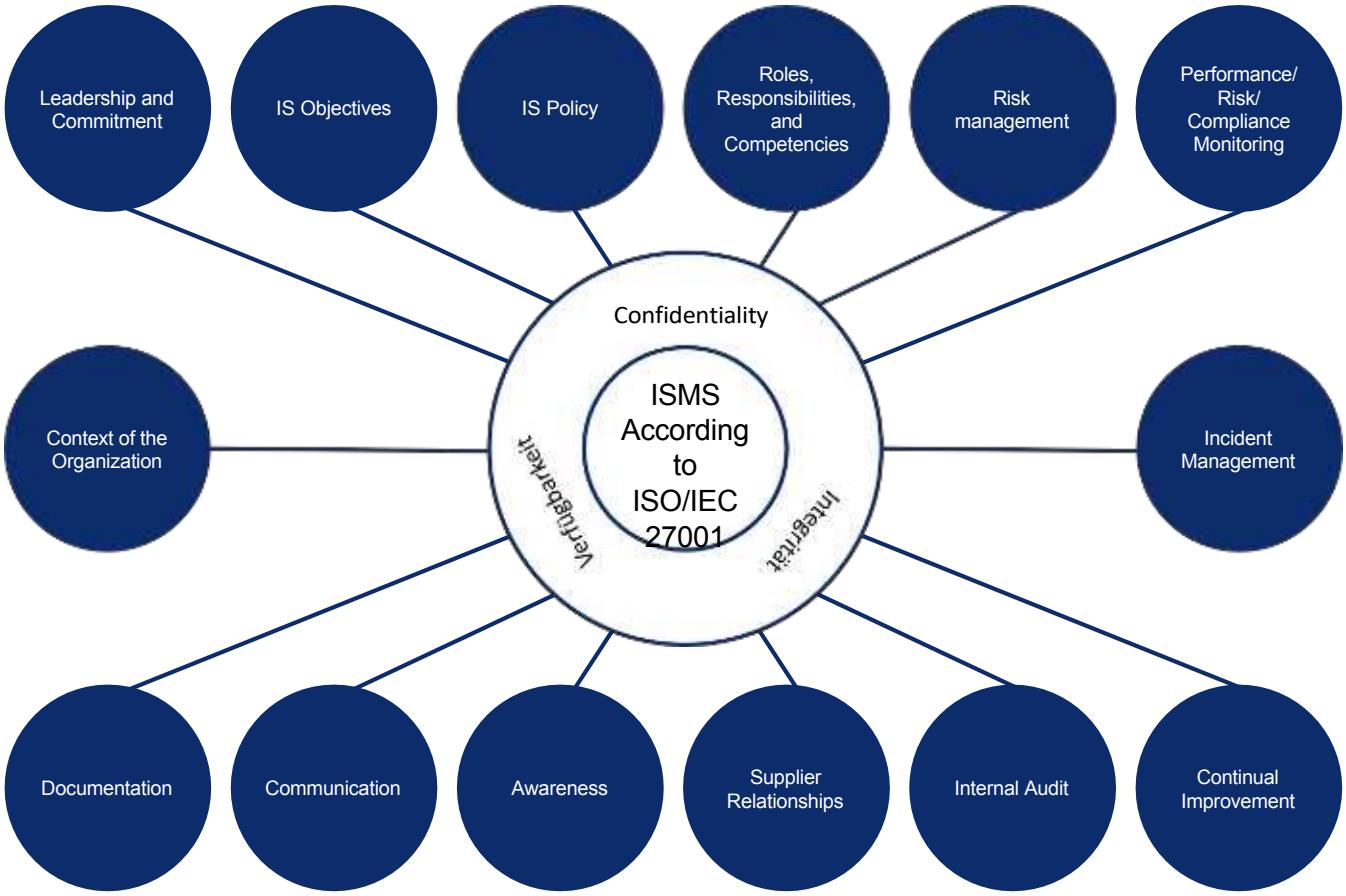


Figure 2: Building blocks of an ISMS according to ISO/IEC 27001:2022

In the following chapters, the key success factors for standard-compliant and proven implementation are outlined for all components.

Since this guideline is also intended to provide practical assistance, the explanations of the building blocks go beyond the purely normative content of ISO/IEC 27001:2022 (or ISO/IEC 27002:2022). Conversely, this also means that not every reference in this document is equally "suitable" for every ISMS or for every organization.

The establishment of an ISMS, whether for self-commitment or with the intention of certification, is an ambitious project that - like any other project - requires "smart "[1] goals, sufficient and expert resources, a suitable project manager, and a motivated and qualified team. In addition, the constant and visible support of top management is crucial for successful project completion and the subsequent transition to ISMS operation.

In addition to assistance, the implementation guide also includes references to further norms, standards or other helpful sources, whereby these are then identified as such.

2.2 Chapter structure

The individual chapters each have the same structure and are divided into the following three sections:

- **Success factors from practice**
  Presentation of - from the authors' point of view - essential Success factors for the establishment and operation of an ISMS according to ISO/IEC 27001:2022
- **Documentation requirements**
  Presentation of documentation requirements, both from a normative point of view as well as from a practical point of view.
- **References**
  Indication of the section relevant to the subject area. numbers from ISO/IEC 27001:2022 as well as further source information, if required and meaningful

2.3 Conventions

For better readability, the gene- rical masculine is used in these guidelines. Unless otherwise indicated, the personal terms used refer to all genders.

Where the terms *"standard"* or *"norm" are* used without further specification, they always refer to the ISO/IEC 27001:2022 standard.

The term *"chapter"* is used when referring within this guide, the term *"section"* is used when referring to the standard.

The term *"Annex"* is used when referring to Annexes of this Guide, and the terms *"Annex"* or *"Annex A" are* used when referring to Annex A of the standard.

The terms *"organization"* and *"company"* each refer to the institution or the area within which the ISMS is implemented. The terms are used synonymously in the guide.

Abbreviations used in the document and further definitions of terms can be found in the glossary in Chapter 5.

1SMART : specific, measurable, accepted, realistic, scheduled.

3 Building blocks of an ISMS according to ISO/IEC 27001:2022

3.1 Context of the Organization

One of the first tasks in implementing an ISMS is to define the specific scope of the management system and to perform a requirements and environment analysis with respect to the organization and its stakeholders. By considering the context of the organization, an organization can ensure that its information security measures are adapted to its specific needs and circumstances and are therefore effective. ISO/IEC 27001 therefore requires organizations to carefully analyze and incorporate the organization's context into their information security planning and implementation.

Determination of the scope

According to the standard, the scope must be documented and describes the scope of the ISMS within a company, i.e., it defines the boundaries and defines which assets (processes, business units, locations, applications, etc.) are within and which are outside the scope.

The identification of the scope is usually performed with the help of an environment and requirements analysis.

- The scope document is essentially a document for the stakeholders of the management system and should be be made available to them upon request, as this is the only way for stakeholders, e.g. customers, to check whether the processes, infrastructures, topics or requirements relevant to them are covered by the ISMS.
- In practice, organizations often refer to any existing ISO/IEC 27001 certificates when making inquiries, which are then - on closer inspection - are often not relevant or sufficient for the request, since the requested process is not or only partially covered by the ISMS. To avoid unpleasant surprises, the scope document or a *precise* description of the scope should therefore always be requested in addition to a certificate.
- Another relevant document for illustrating the scope and extent of an ISMS is the normatively ge- Statement on the applicability of the standard (Statement of Applicability, SoA). The SoA documents the justified decisions on the implementation of the measures (controls) from Annex A, i.e., whether the respective measure is applied within the ISMS or not, including the respective justification for the application or non-application.
- It is customary for the information security policy to define the scope, at least roughly, of the information. is outlined. In contrast to the scope document, the security policy and the SoA are generally internal documents and are not intended to be passed on to external parties. However, attention should be paid to the exact scope definition and the contents of the SoA in the context of service provider relationships and, if necessary, service provider audits.

Environment analysis

The environment analysis serves to integrate the ISMS into the overall environment for the scope in question. In addition to the organizational and technical interfaces relevant for the ISMS, it should also describe the conditions typical for the industry or location. The internal environment, e.g. other management systems (ISO 9001:2015, ISO 22301:2019, etc.), interfaces with other important departments such as risk management, human resources, data protection, facility management, auditing and legal, if not part of the present scope, as well as the external environment, e.g. important suppliers and service providers, strategic partners and, if applicable, other organizations, must be considered.

Requirements analysis

The persons responsible for the management system need a clear overview of which stakeholders exist and what requirements they have for the organization and the management system.

The requirements of interested parties may include legal and official requirements (e.g., EU GDPR, UWG, TMG, regulatory authorities), but also contractual obligations, for example. The organization itself (or possibly a higher-ranking organization in the hierarchy) may also have decision-making and/or directive powers, which must be taken into account accordingly.

Success factors from practice

Since defining the scope is the first and decisive step in setting up and operating an ISMS, this phase should be carried out with particular care. Understanding the context is the basis for all further actions (e.g., structure and process of the risk analysis, organizational structure, definition of work packages and their prioritization, project planning) and is also an essential prerequisite for estimating the feasibility and the effort (resources, budget, time) for the development and subsequent operation of the ISMS.

- In ISO 31000:2018, section 5.4.1 "*Understanding the organization and its context*" lists are offered, with which the completeness of the representation can be achieved.
- The level of detail required to define the scope is usually derived from the internal and external requirements for the organization's information security.

  In practice, it has proven helpful to describe the areas significantly affected by the ISMS in sufficient detail in the scope, since this description is an important control tool and will be relevant for strategy decisions and (subsequent) votes.
- The identification of stakeholders (and their requirements) required by section 4.2 of the standard. must be carried out carefully and comprehensively in any case, because only in this way can clear objectives and contents of the ISMS be defined and the best possible benefits achieved. Examples of stakeholders are: Owners, shareholders, supervisory board, works council, regulatory authorities or legislators, customers, clients, suppliers or subcontractors, service providers, employees, etc.
- Business plans, contracts, etc.can be used as the basis for determining relevant internal and external requirements. such as the requirements of supervisory authorities and legislators for the business processes concerned. In practice, this is often done by a compliance or IT compliance function, which can support the collection of requirements.

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Scope of the ISMS (Section 4.3)
- Applicability Statement (Section 6.1.3 d)
- Overview of all relevant legal, regulatory and contractual requirements, which have an influence on have the information security strategy and ISMS (Section 18.1)
- Overview of all stakeholders relevant to the specific scope of the ISMS.

In addition, the following document has established itself in practice as being target-oriented:

- Interface agreements between the ISMS area and the internal departments supporting the ISMS. areas (to ensure that the cooperation with the internal area is in accordance with ISO/ IEC 27001:2022 and the relevant IS requirements of the organization). Example: Interface agreements with the HR area.

References

ISO/IEC 27001:2022 - Sections 4.3 and 6.1.3

ISO/IEC TR 27023:2015

ISO 22301:2019

ISO 31000:2018

ISO 9001:2015

3.2 Leadership and Commitment

A successful ISMS is implemented using a top-down approach and establishes a link between business objectives and information security by taking into account the requirements of the stakeholders on the one hand and reducing the risks affecting the operational business processes to an appropriate level using effective measures on the other.

In order to fulfill this task, the business objectives and requirements must be known, and appropriate organizational conditions must be created, such as the introduction or adaptation of risk management processes in the organization.

At the latest when it comes to the necessary adaptation of organization-wide processes, leadership (in the sense of setting a direction and vision), approval and support (leadership and commitment) by the management level are unavoidable, as the processes introduced by the management system otherwise have no binding character and thus no value.
u. may not be accepted. Managers are therefore responsible for this, which is also described as "tone from the top" in view of their role model function.

The standard correctly requires explicitly that top management must demonstrably assume overall responsibility for information security within the organization. It must also communicate the importance of an effective ISMS and compliance with the requirements of the ISMS to the employees concerned. This is usually done via the so-called Infor-

mation Security Guideline (cf. *Information Security Policy* in chapter *3.4 IS Policy*) as well as via a user policy.

- Under the heading of (IT) governance and in connection with the responsibility of the executive board
  For strategies, the demonstrable assumption of overall responsibility, particularly in regulated areas, is also increasingly required by the relevant supervisory authorities[1].

Success factors from practice

Definition "Top Management

Top management" refers to the management level that is responsible for controlling the organization to be protected by the ISMS and decides on the deployment of resources.

- In the case of large companies, the standard does not necessarily define "top management "[2] as the highest level of management.
  level of the entire corporate group (e.g., group management board). It can also be a local management or division management that is responsible for the ISMS. The concrete scope of the respective ISMS is always decisive.
- In the case of external certification audits, it is possible that the certification body nevertheless requires the inclusion of the
  The certification body should therefore clarify this point in advance with the certification body when certification is sought. For this reason, it makes sense to clarify this point with the certification body in advance if certification is being sought.

Tasks/responsibilities "Top management

ISO/IEC 27001:2022 requires top management to set a clear example with regard to information security. In practice, this includes not only a visible commitment to information security, but also the

- exemplary compliance with information security requirements,
- sufficient and traceable provision of resources,
- Demanding a role model function from the other management levels,
- Consistently address and respond to nonconformances,
- Self-commitment to continuous improvement.

The central tasks of top management in the context of ISMS are:

- Assumption of overall responsibility for information security
- Definition of the information security strategy and the concrete IS objectives (see chapter *3.3 IS Objectives*)
- Definition of decision criteria and principles for risk assessment and treatment and introduction of ent-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 Continual Improvement*)
- Provision of the necessary human and financial resources for setting up the ISMS and for implementation
  the information security strategy
- Be visible in awareness events or measures (e.g,lead video message).

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Section 9.3 *"Management Review"* requires documentation of the review of the ISMS by the top management.
  management, including decisions regarding changes and improvements to the ISMS. These can be recorded as measures in the risk treatment plan.
- In the management review, results, such as decisions on opportunities for continuous improvement, must be
  The data is stored as documented information.

In addition, the following documents have proven to be useful in practice:

- Derivation and assessment of current risks from identified deviations between strategic IS objectives
  and degree of target achievement, ideally as a risk management plan.
- Evidence to report to senior management,
  z. e.g. in the form of presentations, protocols or re ports

1 Circular 10/2021 (BA) - Minimum Requirements for Risk Management - MaRisk *(https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/2021/rs_1021_MaRisk_BA.html).*

2 See chapter 3.1 *Context of the Organization and ISO/IEC 27000:2018,* Clause 3.75.

- Reporting on the implementation status including its effectiveness control for defined measures (esp.
  when these are overdue) from audits, risk treatment, incidents or continuous improvement

Note: In the context of management responsibility, there are various possibilities for documentation. The examples listed above are suggestions for possible records that help to ensure the traceability of reporting and decision making. Each organization must find the form and frequency of documentation that is right for it.

References

ISO/IEC 27001:2022 - Sections 5.1, 9.1 and 9.3, 5.36

3.3 IS Objectives

The ISMS as a whole contributes to protecting and maintaining the required confidentiality, integrity and availability of the business processes and the information processed therein. The business objectives defined by the company management serve as the basis for the design or definition of the IT objectives and specific information security objectives (IS objectives) and the resulting measures.

Success factors from practice

Since the objectives and principles of the ISMS should be derived from the organization's overall business objectives, failure to achieve the IS objectives can have a direct impact on the achievement of the business objectives. Therefore, it is essential to define appropriate and measurable IS objectives and their implementation.

- The IS objectives must be consistent with the contents of the essential protection objectives (confidentiality, integrity, ver-
  The IS *policy* is based on the IS policy (see also chapter *3.4 IS policy*).

- The IS goals should always be aligned with the overarching corporate goals and should be regularly reviewed with regard to their achievement.
  be checked to ensure that they are up to date and appropriate. This makes it possible to integrate information security requirements into operational business activities in such a way that they are not necessarily perceived as an additional (or possibly even disruptive) expense and the topic of information security becomes an integral part of work processes.

- The company's safety requirements and the results of risk assessments (see Chapter *3.6 Risk Management*) provide a further basis for the selection and definition of IS goals.

- When planning IS goals, it should be determined how these goals are to be achieved. This also includes the de
  definition of the prerequisites for realization. In addition to the essential activities for achieving the goals, the necessary resources and responsibilities as well as a time frame and a procedure for evaluating the realization must be defined. In practice, this is often done by direct reference to planned and ongoing projects. It is crucial that non-functional requirements - and security requirements are non-functional in t h e majority of cases - are taken into account from the outset and integrated both in the planning of projects, products and systems and in the further training of employees ("awareness training").

- When formulating IS goals, care must be taken to ensure that only genuine and long-term goals/
  The targets are described and no operational technical/organizational measures necessary for the achievement of the targets are described.

- As with any formulation of goals, it is advisable to formulate "smart "[3] goals when setting IS goals.
  and to coordinate these with the relevant levels of responsibility.

- The degree of achievement of the information security objectives should be measurable. Ideally, the measurement can be carried out by
  KPIs defined in advance. Practical support for this task is provided, for example, by the ISACA practice guide "Assessing the performance of an ISMS using key indicators" or COBIT 2019 Focus Area: Information Security.

- The formulation of meaningfully measurable goals and the implementation of the measurements required to achieve them are
  In practice, this is quite a challenging undertaking. It is therefore advisable - especially at the beginning of an ISMS implementation - to initially define a small number of IS objectives that are meaningful for the respective organization and balanced in terms of implementation effort and benefits.

- The measurability of IS goals is "only" supported by the standard if there is a corresponding practical implementation.
  practicability is required. In practice, "if practicable" is generally understood to be "softer" than "if possible". This does not mean that measurements are not a normative requirement, but that the practicability of carrying out measurements must always be included in the design (see Section 6.2 b).

3 SMART: specific, measurable, accepted, realistic, scheduled.

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Documentation of IS targets must be maintained.

In addition, the following points have established themselves in practice as being target-oriented:

- IS objectives are usually part of the IS guideline and can also be formulated as part of the IS strategy.
- An implementation plan that describes how IS goals will be achieved through specific projects.
- The degree of implementation of the IS goals is shown by key figures (see chapter *3.7 Performance/Risk/Compliance Monitoring*).

References

ISO/IEC 27001:2022 - Section 6.2 COBIT 2019 Focus Area: Information Security

ISACA Chapter Germany e.V., Practice Guide "Assessing the Performance of an ISMS through Key Indicators".

3.4 IS P olicy

The (top) management responsible for the organization must define an information security policy that documents the organization's strategic decision to implement an ISMS and, in particular, includes a commitment to comply with information security requirements and a commitment to continuously improve the ISMS.

The guideline must be suitable for the organization's purpose and must encompass the intended principles and objectives of the ISMS as well as the organization's information security goals in general.

Success factors from practice

The guideline represents an important tool for the organization, through which the responsible management can communicate the importance of both an effective ISMS and compliance with the ISMS requirements. In addition, the guideline sets out the key strategic and tactical objectives to be achieved with the help of the ISMS. Ideally, the implications and requirements for the respective personnel and business units within the scope are also outlined.

Furthermore, the responsible management should describe the established ISMS, including its roles and responsibilities, in sufficient brevity in the guideline. The following aspects should be taken into account:

- The IS guideline must be approved by the highest management level (top management) and submitted to the responsible
  The Supervisory Board is responsible for the preparation of the consolidated financial statements.
- The IS guideline must be available as documented information and must be subject to a comprehensible document management.
  subject to the risk of changes in the market.
- The IS guideline may include a reference to the company's goals and other relevant subject-specific goals such as
  include the IT goals.
- The language of the IS guideline must be consistent with the company's practices and reflect the importance of dokuments in the best possible way.
- Within the framework of employee sensitization, it must be ensured that all employees concerned within the
  know the IS guideline. It must be communicated to the employees concerned and, if necessary, also be made available to the stakeholders (see chapter *3.10 Competence*).
- In order to achieve the goals in practice, it is important that the individual employees are aware of their individual ver-
  The employees are aware of their responsibility and personal involvement in processes in the context of information security and are familiar with the associated concrete requirements (which are derived from the IS Guideline and are reflected, for example, in topic-specific guidelines and work instructions).
- The IS guideline should not be mixed with more extensive documentation and implementation requirements.
  such as the contents of security concepts or manuals. However, the guideline (or other relevant high-level documents of the ISMS) may very well be referred to in such "downstream" documents in order to achieve consistency in the "chain of requirements".
- Depending on the approach chosen for the ISMS and the existing structure and work organization within an organization, the ISMS may be
  ganization, it may b e useful to use the IS guideline as an
  The IS strategy should be designed as a "powerful", i.e. comprehensive, overall document on the topic of information security or, if necessary, as a specific "anchor" or "starting point" for the topic, which in turn is completed by further detailed documents. In both cases, it is important to use wording and scope appropriate to the goals of the IS strategy.
- If the ISMS documentation is divided into a main document and further detailed documents, a breakdown of

It can also be useful to divide responsibility in favor of flexible change management. For example, the IS guideline is the responsibility of top management, while the detailed documents can be answered by the information security officer or the responsible departments.

- Although a large number of templates and text modules can be accessed in the appropriate search
  it is recommended to create the IS guideline as a new/own document that covers the individual requirements of the organization in the best possible way. Templates can provide ideas and suggestions for structuring and possible content. However, it is crucial for the success of the implementation and the identification of the employees with the topic of information security that the guideline is visibly oriented to the company's and subordinate specialist objectives and that the core statements allow the reader to recognize a reference to the organization concerned.

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Information security guideline (see section 5.2 e)

In addition, the following documents have proven to be useful in practice:

- Topic-specific information security guidelines (see Annex 5.1)
- Accompanying documents and organizational charts, for example to clarify the organizational structure in the
  Context Information security (if not included in the guideline)

References

ISO/IEC 27001:2022 - Section 5.2

3.5 Roles, Responsibilities and Competencies

According to section 5.3 of ISO/IEC 27001:2022, the organization must define the roles required for an effective ISMS and their responsibilities for establishing, maintaining and continuously improving the ISMS. In particular, the necessary resources must be identified and made available (see ISO/IEC 27001:2022, section 7.1).

In this context, management must also assign and communicate the responsibilities and authorities for tasks relevant to information security. Care should be taken to ensure that the responsibilities of the roles are clearly regulated and defined.

and any conflicts of interest are avoided (e.g. with the aid of a RACI[4] or SoD[5] matrix).

Success factors from practice

Concretization of the roles within the ISMS organization

At a minimum, the role of an information security officer (ISO) or chief information security officer (CISO) should be established, although the requirement described in the standard refers to all responsibilities and authorities relevant to information security (see Section 7.2 a). Furthermore, the roles of risk owner and asset owner must be defined and established within the ISMS.[6]

In the context of information security, other roles such as security administrators, internal auditors, etc. must of course be defined and described.

- The role description of the CISO/ISB must also include the necessary competencies (experience, training, schooling, etc.).
  The job description or a letter of appointment listing the tasks assigned should be used for this purpose. For this purpose, it is advisable to refer to a job description or a letter of appointment listing the assigned tasks.
- Conflicts of interest that should be avoided in practice at all costs:
  - Information Security Officer (ISB or CISO[7]) and IT Manager/CIO8
  - Data Protection Officer (DPO) and IT Manager/CIO
  - Internal ISMS auditor and IT administrator
- The two roles of ISB/CISO and DPO can, under certain conditions, also be used in practice in perso
  nal union are exercised by one employee. However, this combination is also associated with certain (unavoidable) potential conflicts. For example, the DPO is protected by law with regard to his actions and is subject to a duty of confidentiality. However, he cannot automatically transfer this protection or this duty to the role of the CISO. There is also a legal discussion regarding the guarantor obligation of the CISO or the compliance officer, etc. This does not apply to the DPO. This does not apply to the DPO. A personal union of these tasks can therefore, in the worst case, result in a substantial conflict of interests.

4 RACI: Responsible (responsibility for implementation), Accountable (overall responsibility), Consulted (professional expertise), to be Informed (right to information), see also glossary.

5 SoD: Segregation of Duties, see also glossary.

6 See section 6.1.2 c and Control A.5.9 "Ownership of assets".

7 CISO: Chief Information Security Officer.

8 CIO: Chief Information Officer.

conflict and should therefore be analyzed and weighed up in detail.

- Depending on the size and business activities of the organization as well as the concretely chosen scope of the ISMS
  The combination of the roles of DPO and CISO can also result in synergies that would not exist if the roles were separated (e.g., with regard to information flow, overview and design of measures). However, on the one hand, it must always be carefully checked whether the candidate in question has the necessary professional and personal competencies and can actually fulfill the workload in t h e two areas. On the other hand, as already explained, it must be checked in detail whether the conflicts of interest that may arise are "manageable" and would not lead to any serious disadvantages in the performance of (one of) the two functions.

- Another example of possible conflicts of interest between the DPO and the CISO relates to the collection and training of DPOs.
  evaluation of traffic and log data. While the DPO will usually only permit the collection and analysis of personal or related data under very specific conditions and for a specific purpose, the CISO would like to make the best possible use of technical measures to increase the level of security (preventive protection) and to detect and evaluate potential damage events (detective protection).

The organization must ensure that all persons have the required competencies through appropriate education, training or experience. The organization must be able to provide evidence of the achievement of competencies, e.g. by means of corresponding further training certificates in the personnel file (training histo- ry) of the respective employee (cf. Section 7.2 d).

- ISO/IEC 27001:2022 provides a rough framework for the security organization of companies (e.g., top-
  management, risk owner, auditor), but does not describe in detail how roles and responsibilities should be distributed in practice.

- It has proven advantageous to select exactly the right employees to fill the required roles within the ISMS.
  The CISO/ISB must select employees who already have an "innate" affinity for the topic of information security or who have sufficient intrinsic motivation. In addition to specialist knowledge, the CISO/ISB in particular requires social skills, goal-oriented communication, integrity, the ability to convince others and successful conflict management. Many of the tasks that arise in connection with the implementation of the information security strategy and (sometimes
  The consequences of the measures, including those that are unpleasant or unpopular, cannot otherwise be satisfactorily resolved.

- In addition, one of the most important characteristics of a CISO/ISB is the ability to distinguish between business objectives and business processes.
  and compliance requirements on the one hand and information security risks and measures on the other.
  to be able to "translate".

- The role of the CISO/ISB requires leadership competencies and should be equivalent in the company to the status of management.
  be on an equal footing with other employees.

- Examples of organizational structures with regard to information security can be found, among others, in " COBIT 2019
  Focus Area: Information Security" and the BSI Standard 200-2 - IT-Grundschutz-Methodik. This describes, among other things, the roles and responsibilities of the CISO, the control committee, the information security manager, the roles in the risk management process, and the functional data owners.

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Proof of competence (section 7.2 d)

In addition, the following documents have established themselves in practice as target-oriented:

- Role descriptions, including the necessary re- porting to top management (see section 5.3 b)
- Job profiles/appointment letters
- Design of the strategic and operational cooperation between the DPO, QMB and CISO.

References

ISO/IEC 27001:2022 - Sections 5.3, 7.1 and 7.2 COBIT

2019 Focus Area: Information Security

BSI Standard 200-2 - IT-Grundschutz Methodology

3.6 Risk Management[9]

An IS risk describes the possibility that a specific threat exploits vulnerabilities of an information system, an application system, or (parts of) the IT infrastructure, which constitutes a breach of information security (confidentiality, integrity, or availability) and thus leads to a negative impact on, among other things, business operations.

9 This chapter refers exclusively to risk management in the context of information security.

The Group's financial performance, financial targets, reputation, or goodwill are all affected by this.

IS risk can generally arise from various sources, such as errors in the configuration or maintenance of systems, human error, cyber attacks, natural disasters, or other unforeseeable events.

IS risk management is an important aspect of corporate governance in general and IS management in particular. IS risk management is an overarching process within a management system which, in the case of an ISMS, contributes to the systematic recording, assessment and transparent presentation of risks in the context of information security and is intended to ensure an *acceptable level of security* or a sustainable improvement in the existing *level of security* within the scope of the ISMS.

The aim is to reduce the identified risks and avert intolerable damage to the organization under consideration or to reduce them to such an extent that an acceptable level is reached for the company. What is considered to be *acceptable* must be decided by the respective persons in charge in the respective context, sometimes also in the respective situation. In addition, there is the decision on how to deal with the identified and assessed risks.

In summary: Intolerable damage to the organization in question must be averted or reduced to a level acceptable to the company.

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

- Early identification and remediation of information security risks
- Establishment of uniform assessment methods for identified risks
- Clear assignment of responsibilities when dealing with risks
- Standardized and clear documentation of risks, including their assessments
- Efficient handling of risks[10]

10 For example, by adapting the security strategy or implementing appropriate security measures.

Basics of IT risk management and procedure

How do risks arise?

Risks in the context of information security arise inherent in the use of IT systems and (emerging) technologies, among other things. Since information security must always be viewed holistically according to ISO/IEC 27001, there are other sources of risk that (can) affect an organization's information/data and arise, for example, from the following influencing factors:

- Data exchange within and outside the organization
- Adaptation of internal organization and cooperation (especially in larger companies)
- (Existing) systems and applications that cannot be updated or replaced
- Cooperation with external partners/service providers
- Remote access to the corporate network (e.g. from partner companies and manufacturers)
- Natural phenomena/natural disasters
- Sabotage and white-collar crime
- "Human risk factor" (e.g., social engineering)
- Use of new types of systems and technologies (e.g. cloud and mobile devices)
- Entering new markets (geographically and product-wise)

Although all sources and influencing factors must be considered, each organization must define its own risk management priorities based on its business activities and the resulting internal and external requirements.

- Efficient risk management can only take place if first the risk exposure and the environment of the respective business activity must be analyzed. In order to know where to "look" for risks, it is necessary to know which risk areas are present overall and to assess them. A good starting point for this is, for example, a process map or an environment analysis (see chapter *3.1 Context of the Organization*).
- To support the formulation and design of the risk assessment process, for example, the ISO/IEC 27005 can be consulted. In addition to the well-developed main section, the appendices in particular also contain valuable information on implementation.

Detection and assessment of risks

Before the concrete identification and treatment of risks can begin, both the ge- nerally formulated risk assessment process and the company-wide or ISMS-wide risk acceptance criteria must be defined in coordination with the highest management level (top management) (insofar as these cannot or must not already be adopted from a higher-level risk management system).[11]

The risk assessment process includes the following:

- Methods for risk identification
- Criteria for the assessment of risks
- Risk Acceptance Criteria

Apply methods for risk identification

Identifying relevant risks usually requires that the views of multiple stakeholders or departments be considered and brought together. Various techniques and methods can be used as tools, such as:[12]

- Interviews
- Scenario analyses/what-if analyses
- Brainstorming
- Business Impact Analyses (BIA)
- Checklists
- Delphi method
- STRIDE Threat Model (Microsoft)

Example

During the risk analysis of a new e-commerce web application, the people involved bring up different risk aspects for discussion. The software developer sees some weaknesses in the selected programming language, which can, for example, be countered by (automatic) code reviews. The IT administrator expresses his concerns about the planned maintenance of the application by external service providers and the access rights to the company network required for this. The data protection officer raises the question of the appropriate protection of personal data and requests a list of the technical and organizational measures to meet the requirements of Article 32 (1) EU GDPR. The information security officer in turn recognizes the scope of the project (impact in the event of availability restrictions or data leakage) and therefore requires a penetration test before going live.

- This example is not taken from a textbook. However, it shows that a risk analysis can also be carried out with the direct for-
  mulation of (counter)measures can go hand in hand.
- If the risk management process is highly dynamic, the direct formulation of (counter-) measures can be a
  The risk management process can also be used to initiate risk management activities in a timely manner. If, on the other hand, the risk management process is implemented with a low dynamic, this can also be deliberately avoided in order to first complete the analysis completely/comprehensively and then define further activities "at leisure".
- With a "compact" or "dynamic" risk management process, which can be swiftly brought to the discussion and
  If the treatment options are not selected, there is a risk that the process as a whole will tend to be reactive and measure-centered, and that the analysis of risks may be neglected as a result.
- Therefore, depending on the size and scope of an organization or a specific project, the most suitable
  nete approach to choose!

Define criteria for assessing risks

The criteria for assessing risks must be formulated in such a way that they can be used for the greatest possible variation of risk types or risk categories. Whether a point model or a catalog of qualitative parameters is used is left to the specific design of the risk management process.

- From a practical point of view, it is advisable, in addition to classical criteria (such as protection requirements for confidentiality/
  integrity/availability, supported business processes, number of users) to provide a set of questions tailored to the organization's business, which can be individually supplemented per use case.
- The assessment of the probability of occurrence (see step 2 "Risk analysis" below) is in practice
  quite challenging. Here it is important that, in addition to the
  In addition to the "look back" (empirical values, comparable events in other organizations, key figures, statistics, etc.), it is essential to also "look forward" in order to be able to take into account previously "unknown" findings and developments that may already be on the horizon (e.g., the emergence of new technologies).

11 In ISO 31000:2018, these activities are described in section 6 "Process".

12 See also IEC 31010:2019.

In other words: "In risk management, success depends on the preparations made.

Set risk acceptance criteria

The definition of risk acceptance criteria is a central task in the risk management process, because this is the only way to achieve the full benefit for the organization of not having to treat all identified and assessed risks "equally" in terms of costs and resources.

- Risk acceptance criteria can take the form of acceptability levels depending on the qualitative and/or quantitative damage potential (e.g. non-compliance, financial damage, damage to reputation, impairment of task fulfillment).
- Risk acceptance criteria may include multiple threshold levels. Each threshold level can be linked to a specific hierarchy/management level, so that acceptance of risks above a certain level is also exclusively by the designated managers within this level.
- For better comparability, qualitative estimation levels can be converted into quantitative (financial) amounts. be networked. However, this is usually only possible in close proximity.
- It can make sense - especially for small and medium-sized enterprises - to use the risk assessment pro- process with a simplified model and then develop it iteratively. For example, in a first step, risks can be collected and initially assessed together with the subject matter experts from the IT department(s) and business department(s) even without a fully elaborated model. The risk acceptance criteria can then be gradually derived from the results and converted into formal criteria at a later stage - after acceptance by the company management.
- When defining risk acceptance criteria, it is necessary to proceed with circumspection and foresight in order to ensure that, on the one hand, the risk appetite[15] of the company (neither too high nor too low) and at the same time ensure the efficiency and effectiveness of the ISMS by minimizing risks. can be identified "across the board" and dealt with consistently according to their assessment and, for example, in accordance with legal or regulatory requirements (not every risk can be given first priority).
- A truly comprehensive risk management system that covers all risks in the con- solidation at any time In practice, the detailed identification and analysis of the information security text in all areas of the company and in all processes is a major challenge.

Orientation to an established risk management process

Once the risk assessment has been defined, the steps of the risk management process follow, each of which is to be carried out iteratively. Following an established process serves transparency and traceability and makes the results of the entire process more reliable. ISO 31000 focuses on the following steps (see Figure 3):

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

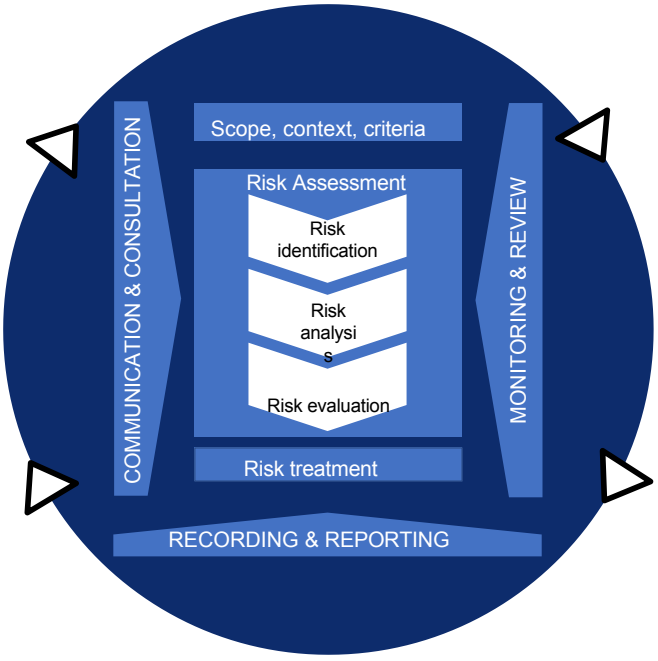


Figure 3: Risk management process according to ISO [3100016]

Step 1: Risk identification

Risk identification is always based on information within the scope of the ISMS (see Section 6.1.2 c).

13 For example, through APTs or zero-day vulnerabilities.

14 Adapted from Confucius, Chinese philosopher, *551 BC †479 BC.

15 The greater the appetite for risk, the more room for maneuver and opportunities are generally available.

16 See ISO 31000:2018.

The identification of specific risks can be derived from the following scenarios, for example:

- Risk analyses
  - For business-critical processes, applications and
    Explicit risk analyses and evaluations are carried out for the processes and systems concerned, with the help of which clear statements can be made about the risk situation and risk exposure of the processes or applications/systems concerned.
  - Within project management, risk ana- lyses (with an adapted scope in each case) should be included as a mandatory element.
- Audits
  - Audits carried out show that safety statuses are being
    The risk that standards and known best practices are not or not sufficiently fulfilled by the responsible parties or in systems.
  - The prerequisite for this is, of course, that audits are also carried out (cf. chapter *3.12 Internal Audit*) and that the audit process includes a clear procedure for handling audit findings (documentation of findings, transfer of findings to the auditee, etc.).
- Operational
  - Through findings in the context of the "normal" ope-
    During the course of the ongoing operation, new, previously unknown risks may come to light, which should/must be reported (promptly) to the risk management team or employee, depending on the risk management process selected.
- Security Incidents
  - Through safety incidents (however the defi-
    nition for "security incident") can, on the one hand, identify previously unknown risks that become visible as a result of the incident. On the other hand, risks that are already known but have not been adequately dealt with or have been accepted so far may actually occur (for example, through active exploitation of an already known vulnerability by an attacker or through failure of a system due to insufficient technical dimensioning).

Step 2: Risk analysis

When analyzing identified risks, both the probability and the possible consequences/consequences should be clearly worked out and presented to the decision-makers in an understandable way.

- In the linguistic formulation of the consequences
  care should b e taken to avoid the consequences for the ge-
  The focus should be on business processes and business activities rather than technical details.
- Standardized evaluation matrices can be used for risk analysis, although depending on the organiza-
  It may make sense to use matrices with an even number of columns (e.g. 4x4). When using matrices with an uneven number of columns/rows (e.g. 3x3 or 5x5), there is a basic risk that the decision often falls on "the middle".

Step 3: Risk evaluation/assessment

The (final) decision on the treatment of identified risks should lie with the risk owner of the respective risk, since he can assess the impact of the occurrence of the risk and bears final responsibility for the business process(es) affected by the risk. As a rule, the risk owner also decides on the provision of resources (e.g., financial resources).

- At this point, it becomes clear how important the identification and definition of the risk owner is for the ge-
  process of risk management.
- In practice, the role of risk owner should be performed by the appropriately designated responsible parties or
  managers of the company (e.g. board of directors, managing director, business manager, division manager, department manager or group manager). In projects, the project manager usually fills the role of risk owner, at least for project-specific risks.

Step 4: Risk treatment

Risks are handled according to the risk map of the respective organization. In the context of information security, the ISO/IEC [2700517] models are particularly suitable as a starting point for modeling risk treatment options (see Figure 4).

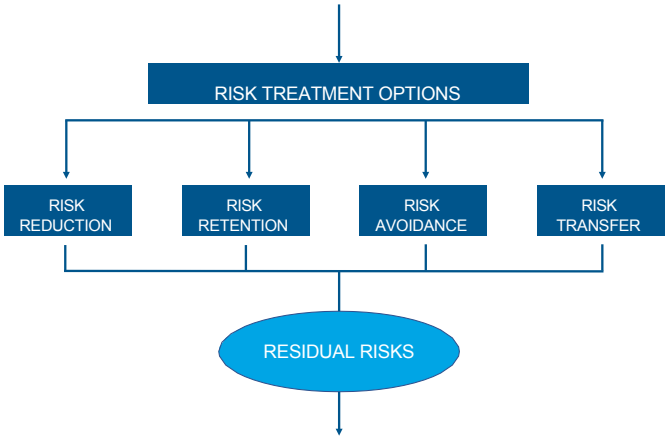


Figure 4: Risk treatment options according to ISO/IEC 27005

17 See, among others, section 8 of ISO/IEC 27005:2022 - "Information security risk treatment".

- Measures for risk treatment can in principle be taken from all sources, but must be
  be aligned with Annex A of the standard and the SoA of the ISMS.

- Risks must be assigned to the associated risk owners. Without dedicated responsible own
  The lack of a "correct" assessment and the long-term successful treatment of identified risks are made more difficult by the lack of a "correct" assessment and the lack of a sustainable successful treatment of identified risks.

- The risk owner is generally the entity that bears the economic impact when the risk occurs.
  must. In many cases, this is the process owner, but depending on the impact and risk assessment, it can also be in higher management.

- Even if risks are caused, for example, by IT systems, the respective parties concerned are ultimately responsible for the risk.
  business units the effects. This means that although (IT) risks must be handled by the respective[18] IT department (responsibility), risk ownership and overall responsibility remain with the business units concerned, which must also decide on the provision of resources (accountability).

- The identification of risks and the identification of the associated risk owners can be carried out separately or in a timely manner.
  are offset from each other.

Documentation and reporting

- It is advisable to keep the results of all risk assessments in a central location, e.g. in the form of
  of a risk register. Although this is not a standard requirement, it helps to evaluate and manage the known risks and their processing status.
  Depending on the size of the organization, tools with different functionalities are required (number of risks, number of users, authorization concept, man- agement capability, online availability, evaluation options, etc.).

- The standard does not require a central risk register. However, it does require that the risk assessment process of
  information security risks leads to consistent, valid and comparable results (see Section 6.1.2 b). Depending on the type and use of the tools employed, the establishment of a register is therefore a logical consequence.

- Since the risk register usually contains sensitive and (strictly) confidential information, an adapted
  rights and roles concept for data access must be created and implemented.

Success factors from practice

- If an overarching risk management system is already in place in the company or the group of companies
  If risk management is not part of operational risk management, IS risk management should be integrated into it (e.g., as part of operational risk management) or at least have defined interfaces.

- Wherever possible, risk management should be process-oriented, rather than focusing on individual asset
  (assets) to the fore. On the one hand, this ensures that risks and hazards are formulated in a (business) process-oriented manner and are thus more easily understood by the risk owners, i.e., usually the process owners, and on the other hand, the potential (damaging) impacts can be determined very accurately.

- The process model for the implementation of projects in the company should be adapted and extended.
  The project team must document the results of the analysis and - depending on the design of the risk management system - report risks that exceed a defined threshold value. The project team must document the results of the analysis and - depending on the design of the risk management system - risks that exceed a defined threshold value must be reported. Formal risk acceptance by the respective risk owner must also take place and be documented in the event of missing measures or risk acceptance.

- Even in the case of (extensive) changes to processes, applications or systems, it is recommended that risk
  introduce analyses and assessments as a mandatory part of change management.

- If nonconformities or vulnerabilities are identified (e.g., through monitoring or other operational
  IT processes such as change, problem or incident management) that cannot be remedied within regular operations or cannot be remedied in a timely manner, these must be assessed in risk management and dealt with by the risk owner.

- Risk analyses and assessments always involve the specialist know-how of the respective process owner.
  The IS officers of the organization can provide support during the implementation. The IS officers of the organization can support the implementation and, for example, record the risks in interviews or workshops and make suggestions for evaluation. A

18 This also includes specialist departments and software development departments, which may be located outside IT, have their own IT risks to answer for and are responsible for their risk handling.

Another method is the use of questionnaires/self-assessments. Depending on the approach chosen, these self-assessments can then be additionally evaluated by a "second set of eyes". It is crucial that there is a formal and pragmatic process that optimally supports the departments and project managers in their work and at the same time ensures that risks are identified at an early stage and dealt with appropriately.

- BSI Standard 200-3 - Risk analysis on the basis of IT-Grundschutz - provides starting points on how to use the information provided in the IT-Grundschutz-Kompendium, a risk analysis can be performed for information processing. However, the BSI methodology requires that the steps of the IT-Grundschutz procedure have first been carried out (including information networking, structural analysis, identification of protection requirements, modeling, IT-Grundschutz check, supplementary security analysis) before it can be decided for which target objects a risk analysis is to be carried out and for which target objects, on the other hand, this is unnecessary.
- The asset worth protecting in the context of an ISMS always remains the information itself. It is the task of the respective responsible parties (company management, management, process owners) to evaluate this asset with regard to its "value" for the company or the respective process. The information asset thus becomes the information value. The task of the risk owners is to establish appropriate, effective and efficient measures within all process steps. Those responsible for the ISMS are the "watchdogs" for the implementation of the information security strategy and are responsible, among other things, for truthful reporting with regard to risk exposure and security incidents.

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Risk assessment process (section 6.1.2)
- Risk treatment process (section 6.1.3)
- Records and results of risk assessments or risk analyses (section 8.2)
- Records and results of risk treatments (Section 8.3)

In addition, the following documents have proven to be useful in practice:

- Records and results of risk assessments and risk analyses

References

ISO/IEC 27001:2022 - Sections 6.1, 8.2, 8.3

ISO/IEC 27005:2022

ISO 31000:2018

COBIT 2019 Focus Area: Information Security

BSI Standards 200-2 and 200-3

3.7 Perf ormance/Risk/Compliance Monitoring

A number of specifications are defined in the context of the ISMS, z. For example, information security objectives or guidelines and concepts for their implementation in practice. It is expected that it is continuously ensured that these requirements are met, which must be ensured by means of appropriate monitoring. "Performance/risk/compliance monitoring" thus also refers to the continuous monitoring and improvement of the information security management system (ISMS).

- Performance monitoring comprises the evaluation of t h e effectiveness of the ISMS in terms of achieving of the security objectives and compliance with the requirements of ISO/IEC 27001.
- Risk monitoring refers to the assessment and monitoring of security risks in the company and in the ISMS (see also Chapter 3.6).
- Compliance monitoring relates to the monitoring of adherence to legal requirements and the regulatory requirements, but also by internal guidelines and standards.

Performance, risk, and compliance monitoring is designed to help organizations ensure that their ISMS is operating effectively and efficiently and that it meets the requirements of ISO/IEC 27001 as well as legal and regulatory requirements. It involves regularly reviewing ISMS processes, procedures and controls to ensure that they meet the relevant requirements.

In order to establish comparability, continuity and traceability, all objectives whose achievement is to be measured by key performance indicators should meet the SMART criteria:

- Specific
- Measurable
- Attractive/Accepted
- Realistic
- Terminated

This ensures that these goals are described accurately, clearly and in a way that everyone can understand.

The information security officer is now in a position to evaluate and control information security on the basis of the various key figures, e.g., with the help of a dashboard view. From the large number of metrics, we focus on the following metric classes with regard to information security:

Key Performance/Risk/Control Indicators (KxIs)

KPI - Key Performance Indicators
A key performance indicator is a value (target/actual comparison) that shows how **successfully** a company implements the relevant measures and the information security processes in relation to achieving the information security objectives. A measure is successful if the desired level of performance is achieved within the specified time and with as little effort as possible.

KRI - Key Risk Indicators
A key risk indicator is a value (target/actual comparison) that shows whether changes in the risk profile potentially exceed the desired tolerance limits and thus jeopardize the achievement of objectives. It is therefore a measure of how **risk-oriented** a company is in implementing the relevant measures.

and implements the information security processes. A situation that exceeds the company's risk appetite is brought back into the acceptable risk range by taking countermeasures.

KCI - Key Control Indicators
A key control indicator is a value (target/actual comparison) that shows how **effectively a** company implements the relevant measures and information security processes in relation to target achievement. A measure is effective if the control objectives are reliably achieved within the desired tolerance limits.

In order to continuously monitor the effectiveness and efficiency of the ISMS processes and the established measures, these indicators should be used in practice (see Fig. 5). They provide information about the performance status of the entire ISMS and serve as triggers for necessary management intervention.

This means recording the actual situation in relation to the target situation described by the specifications and, if necessary, intervening in a controlling manner. These performance indicators are summarized in relation to the corporate goals to be achieved, legal requirements and protection needs.

The added value of KxIs lies in their ability to provide basic statements about the protection system. They serve the

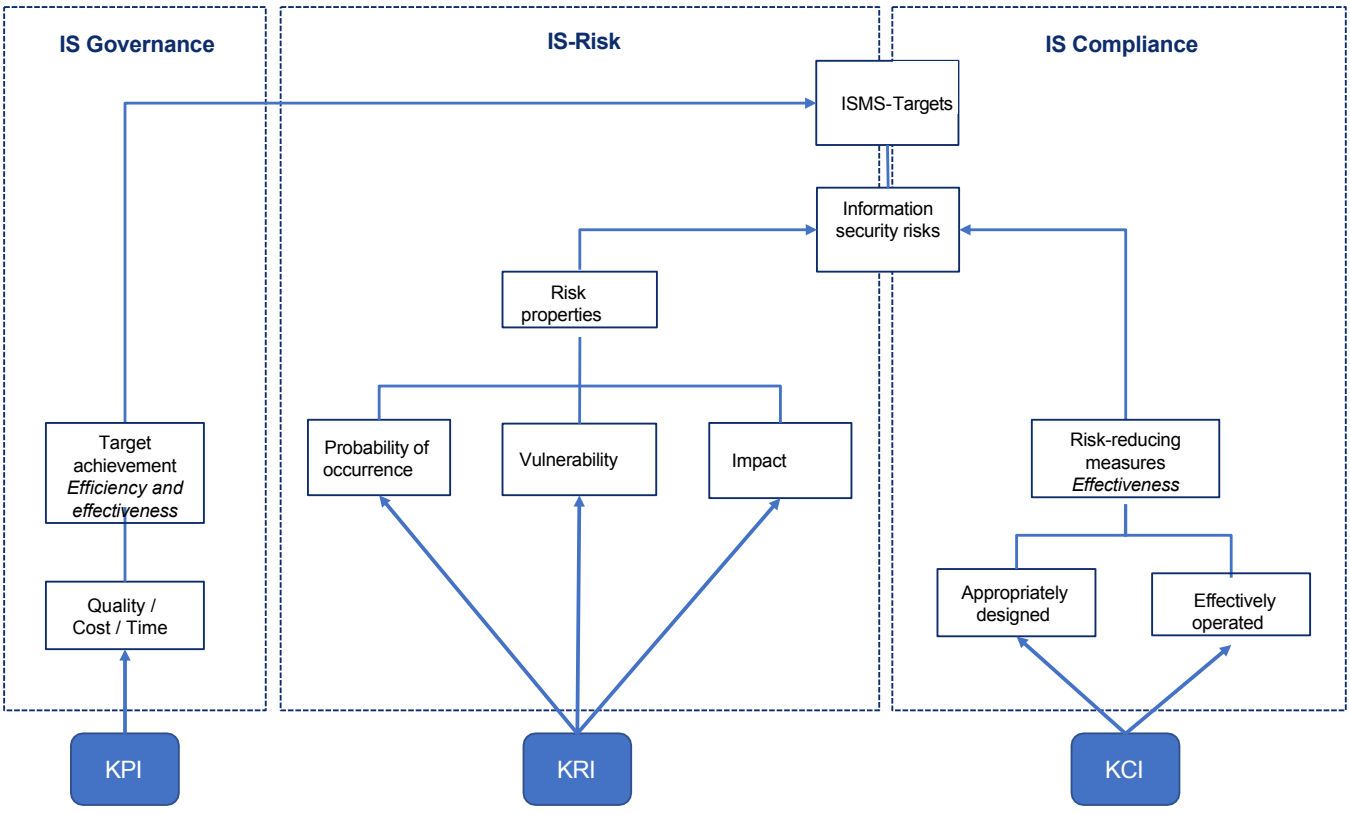


Figure 5: Structure and relationship of KPI, KRI and KCI

management as a comprehensible and understandable basis for well-founded decisions on the management of information security. In addition to the classic performance analyses, KxIs can be used to reveal indications of (new) risks or changes within the risk landscape as well as non-conformities with regard to the implementation of security requirements and guidelines.

Success factors from practice

Key indicators can only be used meaningfully to represent the current situation and control if they meet certain requirements:

- Each key indicator must be measurable, repeatable and comparable, both along the timeline and across industries or at least organizations.
- Indicators should be systematically structured and based on sound and appropriate statistical-mathematical fundamentals with reliable measurements based on a sufficient scope.
- The indicators should be timely and reflect current information. The frequency of data collection The processing and the duration of the processing until the presentation to the management should enable the control, similar to the displays on the dashboard of a car, which tell the "steering" of the system whether all "important" parameters are in the desired, orderly range.
- Performance indicators must be relevant to the goals of information security management, have a controlling effect on the and provide practical support for decision-making.
- The selection of indicators should be risk-based and the cost-effectiveness of data collection should be taken into account. The results must be compared with the informative value and usability for decision-making.
- The selection of KxIs should enable an evaluation of the ISMS as a whole. That is, it is not sufficient, only individual sub-aspects and indicators. Rather, they must be combined into a meaningful whole and capture the performance of the entire ISMS.
- Performance indicators can also be used to evaluate and manage service provider relationships and be included, for example, as part of a contract or in a (security) SLA.
- See also Annex 8.3 *Holistic safeguarding of the Value chain*, page 66

Relevant KxIs for the ISMS

There are many sources of information security performance metrics that offer a huge selection, such as COBIT 2019 for Information Security[19], The CIS Security Metrics[20], or Performance Measurement Guide for Information Security[21], to name a few.

Of course, we would also like to take this opportunity to refer to the ISACA practice guide "Assessing the performance of an ISMS using key performance indicators (for a goal-oriented IS key performance indicator system according to ISO/IEC 27004:2016)".

The specific selection of KxIs should be based on the circumstances of the respective organization, fulfill the quality criteria already described and be continuously optimized.

Below are some examples of such key indicators from the ISACA Practice Guide for Assessing the Performance of an ISMS by Key Indicators:

Key Performance Indicators

- Time required compared to the planned time at the given implementation rate (e.g. 80% of employees) of an awareness campaign.
- Required budget compared to the planned budget for the implementation of an awareness campaign

Key risk indicators

- Percentage of employees clicking a prepared phishing link during an awareness campaign
- Percentage of IT systems with vulnerabilities that were not closed in the designated time window
- Percentage of productive IT systems for which there is no longer manufacturer support

Key Control Indicators

- Ratio of employees trained to date compared to the planned number of employees to be trained in an awareness campaign.
- Number of employees who passed the learning check at the end of the awareness campaign, compared to the number of employees already trained during an awareness campaign.

19 ISACA, COBIT 2019 for Information Security, 2019.

20 The Center for Internet Security, "The CIS Security Metrics."

21 "Performance Measurement Guide for Information Security," NIST Special Publication SP 800-55.

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Documentation of the measurement structure for all KxIs. It answers the following questions:
  - What was measured and evaluated?
  - Which methods were used for measurement, analysis and evaluation and do they lead to reproducible results?
  - When was it measured by whom?
  - When was it analyzed and evaluated by whom?
- Results of the measurements and the management reports derived from them for escalation

In addition, the following documents have proven to be useful in practice:

- All records and evidence that provide information relevant to the context of effectiveness monitoring
  as the organization must maintain documented evidence of monitoring and measured results.

References

ISO/IEC 27001:2022 - Section 9.1

ISO/IEC 27004:2009 - Sections 5, 6, 7, 8, 9, 10 and Annex A

COBIT 2019 Focus Area: Information Security

3.8 Documentation

In the context of documentation, it must be ensured as a central requirement within the management system that (at least) the following aspects are regulated for the ISMS documentation:

- The creation and updating, as well as the approval and, if necessary, communication of documents must be
  run according to a defined procedure (workflow).
- The documents must be clearly identified, e.g. title, date, author, version, version number, version number, version number, version number, version number, version number, version number, version number, version number, version number, version number, version number, version number, version number, version number.
  and an appropriate suitability and fitness for purpose test (QA) and final release.
- Classification of documents or their contents with regard to confidentiality
- Preparation of sufficient and relevant records within the framework of the operational activities for the
  Ensuring traceability

The contents and the level of detail of the documents required by the standard are influenced by the selected scope of the ISMS, the size of the organization, the technologies used and the organizational structure, among other factors, and therefore differ from organization to organization.

The number and type of documents also vary. From a practical perspective, it may make sense for one organization to create a set of (many) individual documents and maintain them granu- lar. For another organization, on the other hand, it may be more appropriate to use a central storage medium that is accessible throughout the organization. In practice, this can also mean using a wiki or another online system as a documentation basis.

If no specific documents are required, the ISO/IEC 27001:2022 standard uses the term "docu- mented information" in connection with documentation and records. In this case, the company is free to decide in which associated documents this information is kept, whereby the term "document" includes any format.

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

- Availability and suitability for use, irrespective of place and time
- Adequate protection, e.g. against loss of confidentiality, improper use or unauthorized access.
  Manipulation/loss of integrity

Success factors from practice

In practice, the fulfillment of the requirement for document control can generally be supported by a document guideline. However, the decisive factor for successful implementation is not the quantity of documentation, but its quality, acceptance and availability as well as its efficient control (keyword: document control).

Practical aspects for the assessment of documentation quality and document control result from the following questions:

- How are contents and changes to the documentation communicated to the affected employees or ge-
  trains?
- How well are employees familiar with the content and how are the requirements of the documents met by
  the affected persons "lived" in everyday life?
- Who knows the filing locations and filing media where the current documents can be found?

- Is the content prepared in a target group-oriented manner and formulated clearly?
- How easy is it for new employees to grasp the contents of the documents and implement them in their own working environment?
  set? What kind of demands are there?
- Are the documents updated regularly or as required? How well do the updates work?
  and the release of the documents?
- Are there dedicated document owners per document?

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist (sections 4-10):

- *Scope of* the ISMS (Section 4.3)
- *Information security po- licy*, section 5.2 e)
- Description of the risk assessment process (*Informa- tion security risk assessment process*, section 6.1.2)
- Description of the risk treatment process (*Informa- tion security risk treatment process*, section 6.1.3)
- *Statement of Applicability* (Section 6.1.3 d)
- *Information security risk treat- ment plan* (Section 6.1.3 e)
- Security objectives (*Information security objectives and plan- ning to achieve them,* Section 6.2)
- Monitoring to achieve the security objectives (*informa- tion security objectives and planning to achieve them*, Absections 6.2 d, 6.2 g)
- *Evidence of competence* (section 7.2 d)
- Evidence of correct execution as well as changes to ISMS processes[22] (*Operational planning and control*, Section 8.1 d; *Planning of* changes, Section 6.3)
- *Results* of the *Informa- tion security risk assessment* (Section 8.2)
- Results of the risk treatment (*Results of the Infor- mation security treatment*, Section 8.3)
- *Evidence of the monitoring and measurement results of* the ISMS,
  Section 9.1)
- *Evidence of* the implementation of audits and their results (*Evidence of the audit program(s) and the audit results*, section 9.2)
- *Evidence of the* results *of management reviews* (Absection 9.3)
- Identified deviations from ISMS requirements and measures to correct them (*Evidence of the nature of the nonconformities and any subsequent actions taken*, Section 10.1 f)
- *Evidence of the* results *of any corrective action* (Absection 10.1 g)

Furthermore, the organization must determine for itself what documentation and records are necessary in addition to what is required by the normative in order to have "sufficient confidence that the processes have been carried out as planned" (see Section 8.1).

The ISMS processes for risk management, incident management and continuous improvement of the ISMS should be visualized using suitable process representations (e.g., event-driven process chains, EPCs) and communicated to the employees in a comprehensible manner using process descriptions and concrete work instructions.

In addition, there are the documents and records from Annex A, provided that these measures are applied in accordance with the "Statement of Applicability".

References

ISO/IEC 27001:2022

3.9 Communication

When operating an ISMS, cooperation with other organizations and departments is required (e.g., suppliers, HR department, legal department, auditing). The main task of the "Communication" module is to determine and describe the need for internal and external communication.

External communication refers to communication with (external) stakeholders and other organizations (see also environment 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 executive board, managers and employees.

An analysis should determine what information needs to be communicated in the context of the ISMS (Section 7.4 a of the standard), by whom (Section 7.4 d), and to whom (Section 7.4 c). In addition, it should be determined when communication is to take place (Section 7.4 b), and

22 In this context, the standard speaks of "documented information to the extent necessary".

via which communication channels/processes (section 7.4 e) this is to be done.

Ideally, the results of the analysis are summarized in a communication plan. This is usually formally developed in five concrete steps (see Figure 6):

Figure 6: Development of a communication plan

- Process and communication interfaces should be clearly defined in terms of efficiency and integrated into the or-
  The information must be integrated into the organizational and operational processes. It must be clearly defined which information must be delivered to whom and by whom at what point in time, for example as part of change or incident management.
- The standard requires that the organization determine internal and external communication in the context of the ISMS.
  It does not explicitly require that this be done as part of an analysis. However, the practical benefit of an analysis is that it can be used to clearly identify which requirements exist for a precisely fitting communication structure.

Success factors from practice

A communication plan, also known as a communication matrix, can look like tables 1 and 2.

Internal communication				
Communication reason	*Initiator*	*Receiver*	*Frequency*	*Medium*
Management review	CISO	Top Management	annual	Management report according to template by mail + presentation
Reporting	CISO	Top Management	quarterly	KPI report according to template via e-mail + presentation
Awareness training	CISO	All employees in the scope	annual	Training (presence/online)
IS Newsletter	CISO	All employees in the scope	on a quarterly basis and on a case-by-case basis in the event of an acute threat	E-mail
Risk Management	CISO	Top Management	quarterly, case-related in case of acute threat, project-related	Balanced scorecard report, via email if applicable.
Security Incident	Support	CISO *(if necessary further according to SIRP)*	case-related	Escalation according to SIRP (Security Incident Response Process)
Security Incident	CISO	Top Management	case-related	E-mail, if necessary verbally
Security incident with personal data	CISO	Data Protection Officer	case-related	E-mail, if necessary by telephone or verbally
Security incident with compliance reference	CISO	Legal Department	case-related	E-mail, if necessary by telephone or verbally

Table 1: Communication plan - internal communication

External communication				
Communication reason	*Initiator*	*Receiver*	*Frequency*	*Medium*
Report Operating Service Provider	Operating service provider	CISO	quarterly	SLA report according to template via e-mail
Externally commissioned CERT/ Vulnerability Analysis	CERT	CISO/IT Manager	weekly/case-related	Report according to contract by e-mail
Security Incident	CISO, if necessary top management	Customers/partners concerned	case-related	according to SIRP, on website, letter, e-mail, telephone
Security incident with criminal background	CISO	Investigative agencies	case-related	according to SIRP

Table 2: Communication plan - external communication

- Once the communication matrix has been worked out, it has been shown in practice that various interfaces betwi- already exist between communication partners and/or departments. Identifying these is an important success factor for efficiently designing communication in the context of the ISMS in the organization. It may make sense to integrate the IS communication plan into an overall communication plan.
- In order to be able to communicate with all levels of the organization, a platform should be provided that- with which the comprehensive security information of the ISMS is accessible to different target groups. Collaboration platforms for better communication or reporting could be e.g. intranet, Confluence, Wiki or similar.

Documentation requirements

According to ISO/IEC 27001:2022, there are no normative requirements for the documentation of the ISMS with regard to communication.

In addition, the following documents have proven to be useful in practice:

- Procedures for internal and external communication
- Communication matrix
- Communication plan

References

ISO/IEC 27001:2022 - Section 7.4

3.10 Awareness

"Information security is the operation of firewalls and antivirus" - this is one of the frequent and major misconceptions that jeopardize the security of information and IT systems of a company, because a large number of of safety-relevant events and safety incidents in operations falls into the categories of "lack of sense of responsibility," "lack of or immature processes," and "inadequate employee training and/or sensitivity."

The creation of a "healthy" risk awareness is therefore an essential component of a practical ISMS that generates benefits for the organization by identifying threats at an early stage, avoiding security incidents and "saving" the effort that would be required to deal with them.

Security awareness is not a matter of course, but must be actively promoted and demanded by the company through appropriate awareness campaigns, including the following important aspects (see Section 7.3):

- Knowledge of the information security guideline and user guideline as well as the relevant information
  The safety guidelines on the part of the recipients of the specifications (employees, managers, external partners) must be ensured.
- The contribution of each employee within the scope of the ISMS should be aligned with the requirements set out in the user guide.
  The materials used for awareness measures ideally support the communication of this content. The materials used for awareness measures ideally support the communication of this content. It is recommended to prove successful communication by means of tests.
- Effects and, if applicable, sanctions for non-compliance with safety regulations should be derived from the materia-
  The information must be provided in the form of the data used in the context of an awareness measure. At the same time, a user's report of a security breach (e.g., whistleblower) due to his or her own misconduct should not generally lead to sanctions.

Success factors from practice

In practice, information security awareness campaigns can usually be divided into different phases. First of all, a needs assessment is carried out, and then an awareness campaign is planned and implemented in line with the target group and on the basis of specific potential threats. Information security awareness should not be seen as a one-off project, but should be established sustainably through mechanisms planned into the campaign. The analysis of the effectiveness of a campaign should be considered in advance. In practice, the following phases have proven to be useful for a security awareness campaign (see Figure 7):

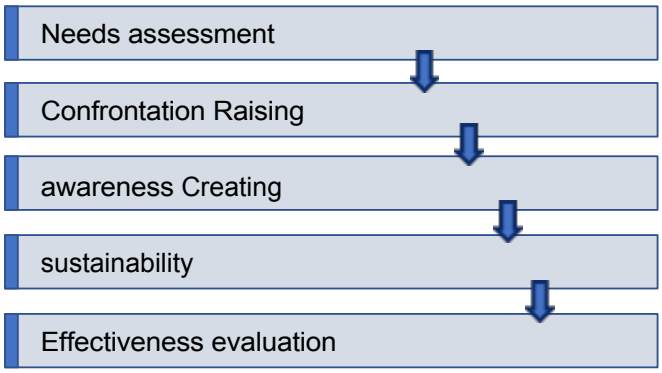


Figure 7: Phase model for security awareness campaigns

Phase 1: Needs assessment (based on hazard potentials)

Successful implementation of security awareness campaigns requires knowledge of the target group and its needs. For this reason, awareness campaigns should always start with a needs assessment.

- Security awareness is useful in all areas of a company, but only in one of the actual areas.
  hazard and to the extent appropriate to the target group.
- Knowledge of safety requirements can be increased, for example, through awareness measures with active participation and parti
  The evidence must be provided in the form of a record of the customer's activities.

Before starting to define and plan awareness measures, a company should therefore think about its individual potential dangers (risks) in relation to the users. It is not very helpful to confront users with hazards and situations that do not apply to their area.

Phase 2: Confrontation with the topic

In the "confrontation" phase, the employees' attention is to be aroused for the topic, consternation is to be generated and acceptance for phase 3, i.e. the actual sensitization, is to be promoted. This is usually best done by directly confronting employees with the topic ("experience-based learning").

- Through personal experience, employees are made aware of their importance for information security.
  sibilized and are normally subsequently grateful and open to further training measures on the subject.

Below are some simulations of attacks to confront employees with the topic:

- Social engineering attacks on employees, e.g. using fake calls to obtain confidential information.
  (such as passwords), and fake e-mails (e.g., requesting password entry into an online system with the ostensible purpose of checking password strength for an upcoming audit).
- Prepared USB sticks should be available within the company (parking lot, meeting room, toilets, etc.).
  The system can generate warning messages that can be registered anonymously and used for evaluation ("I could have been a virus").
- Search waste paper garbage cans or waste paper baskets for confidential documents ("dumpster diving").

Practice has shown that the above-mentioned attack scenarios lead to - in this con- text - "valuable" security incidents and usable information in most companies. The "anonymous" resolution of the action in conjunction with the presentation of possible conse- quences for the company usually provide for a
"Hello-wake-up effect" among employees, which can be used as an introduction to the actual IS campaign ("knowledge transfer"). For ethical reasons, too, it is advisable to carry out simulated "attacks" on employees only after prior announcement and in close coordination with the works council, if one exists, in order to avoid resentment among those affected, which could counteract the desired learning effect.

As an alternative to such campaigns, the "confrontation" can also take place passively, for example at the beginning of a classroom training. Demonstrations could include live hacking sessions, anonymous testing of password strengths, or role plays.

- An essential aspect in this phase is to create a positively designed entry point for the topic and to
  thus the contact with the employees "at eye level

to establish. Despite all confrontation, the basic direction must always be to "pick up" the employees where they are at the moment (What IS requirements already exist? How have these been communicated so far? What incidents have already occurred? etc.), and to actively involve them.

- It is also important to be clear about the framework and to identify any information gaps that may exist.
  cken to know. The scope of the activities performed and information provided must be consistent with the
  The campaign must be balanced against the "absorption capacity" of the addressees. Only in this way can the campaign develop its full effect and be perceived neither as too banal nor as too excessive/overloaded.

Phase 3: Sensitization

The actual sensitization is at best a mix of knowledge transfer, demonstration and active participation of the employees. Various methods can be used to impart knowledge (pre-service training, e-learning, etc.).

The categorization of awareness-raising activities into thematic areas or measures has proven effective, in particular the following:

- **Physical safety/workplace safety**
  - What must be considered when entering the buildings and
    premises be respected?
  - How can unauthorized persons be prevented from gaining access, e.g. incorrect deliveries or an unknown person attaching himself to a group of employees and entering the building unnoticed ("piggybacking")?
- **Privacy**
  - The data protection section should comply with the legal requirements.
    The data must be kept secret, deletion procedures must be in place, and employees must be obligated to comply with them.
- **IT Security**
  - What is important when dealing with IT systems and compu-.
    tern, e.g. handling e-mails, surfing the Internet, handling removable media (CDs, USB sticks), protection and tools against malware?
- **Telephony**
  - What can happen when information worthy of protection is
    tions or processes are disclosed over the phone?
- **Reporting and handling of security incidents**
  - What (central) points of contact are there?
  - What are relevant initial actions?

In addition, particularly vulnerable target groups (e.g., IT administrators, employees and managers with far-reaching access and information rights, mobile employees, but also call center employees or other groups with external contact) must be taken into account in order to weigh up whether they need special training.

Awareness materials should be created and distributed as needed to support the training. These can be, for example, one-page or multi-page brochures or newsletters with training content, but also posters, stickers or other media with a high recognition effect (posters, flyers, videos, etc.).

- Optimally, awareness materials are created by the company's own employees as part of the
  IS campaign. Additional motivation to cooperate can be achieved through an incentive [system23].
- A guiding video from top management can emphasize the importance of
  of the topic with a corresponding request to the co-
  The aim is to emphasize the importance of employees handling information in a mindful manner.

Phase 4: Create sustainability

One-off awareness measures are not sufficient to bring about a sustainable change in behavior among employees. Although it is necessary to carry out extensive initial sensitization, only regular repetition of the topics on the basis of a training plan and regular communication of the key messages in everyday life can ensure lasting awareness. Ways to create a subconscious presence of the topic in everyday life include:

- Regular sending of simulated phishing e-mails (e.g. to reveal access data)
- Publication of current news (e.g. via intranet, employee newspaper)
- Integration of an online quiz on the topic of IS on the intranet or via an app (possibly with incentives)
- Use of a screensaver with appealing safety messages
- Annual implementation of a cyber security month with e.g. internal or external presentations, live hackings

23 Incentive = incentive, performance incentive.

Phase 5: Evaluation of effectiveness

In this phase, the maturity of employee sensitization is assessed at regular intervals. The aim is to create transparency with regard to the maturity level of employee sensitization. Possible KPIs for measurement are, for example:

- Number of safety incidents called out due to misconduct as a proportion of all safety incidents.
  fall
- Number/ratio of click-throughs or password entries to simulated phishing emails.
- Results of a quiz or test on the topic of information security
- Net Promoter Score (NPS) for training content

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Evidence of the competence of employees in the area of application of the ISMS (Section 7.2)

In addition, the following documents have established themselves in practice as target-oriented:

- Awareness/training concept
  - What topics are covered?
  - How are awareness measures implemented, z. e.g. classroom training and/or online training?
  - How are the contents of the information security guideline communicated?
- Awareness/Training Program
  - When are which topics dealt with?
  - Are updates on measures, as required by the standard, provided on a regular basis?
- Training materials that concisely reflect the contents of the information security guideline; and
  point out dangers and weaknesses in information processing
- Proof of participation: names of the persons participating, contents and date of the awareness measure

References

ISO/IEC 27001:2022 - Sections 7.2 and 7.3

3.11 Supplier Relationships

The high level of networking and standardization in information processing have made it necessary to use external service providers.

suppliers is strongly encouraged. Conversely, security risks at the service provider/supplier also have an impact on the company's own infrastructure. This has been demonstrated by a number of high-profile incidents in recent years in which security deficiencies at service providers/suppliers led to data theft or other security incidents at well-known companies.

The term "service provider" or "supplier

In the self-image of the ISO/IEC 27001:2022 standard, the term "supplier" covers a wide range of business relationships with external companies and partners. It includes relationships from the IT environment, such as software manufacturers, IT service providers, outsourcing partners or cloud service providers, but also from other areas. These include, for example, logistics, utilities, facility management, cleaning service providers and many others.

The requirements of ISO/IEC 27001:2022 focus on various protective measures, such as the definition of processes and procedures (section 5.19) and the agreement of contractual regulations with the supplier (section 5.20), e.g., connection to logging or security logging, CERT connection, reporting channels for security incidents, integration into an existing identity management system. Risks from the supplier's ITC infrastructure, supply chains and other subcontractors (Section 5.21) as well as regulations for monitoring and modifying service provision (Section 5.22) must also be taken into account.

A topic-specific policy should be established for the use of cloud services and processes developed for the entire lifecycle of the service (Section 5.23). In this way, relevant aspects of information security are addressed from procurement, use, management and exit from the cloud service.

ISO/IEC 27036 and other relevant standards

The ISO/IEC 27036 standard "Information security for supplier relationships" offers a much more detailed view. It addresses the necessary processes and describes the activities required in the respective process. Certification according to this standard is not possible, but a common terminology is created which, among other things, provides many concrete aids for implementation.

Figure 8 shows an overview of the standards that are relevant in this context, divided into overview, requirements and guidelines, as well as supplementary documents that focus on processes and techniques.

In regulated industries, further specific requirements may have to be taken into account, for example MaRisk AT 9 for banks. In addition, ISO 28001 is increasingly being used.
"Security Management Systems for the Supply Chain" as a Be-

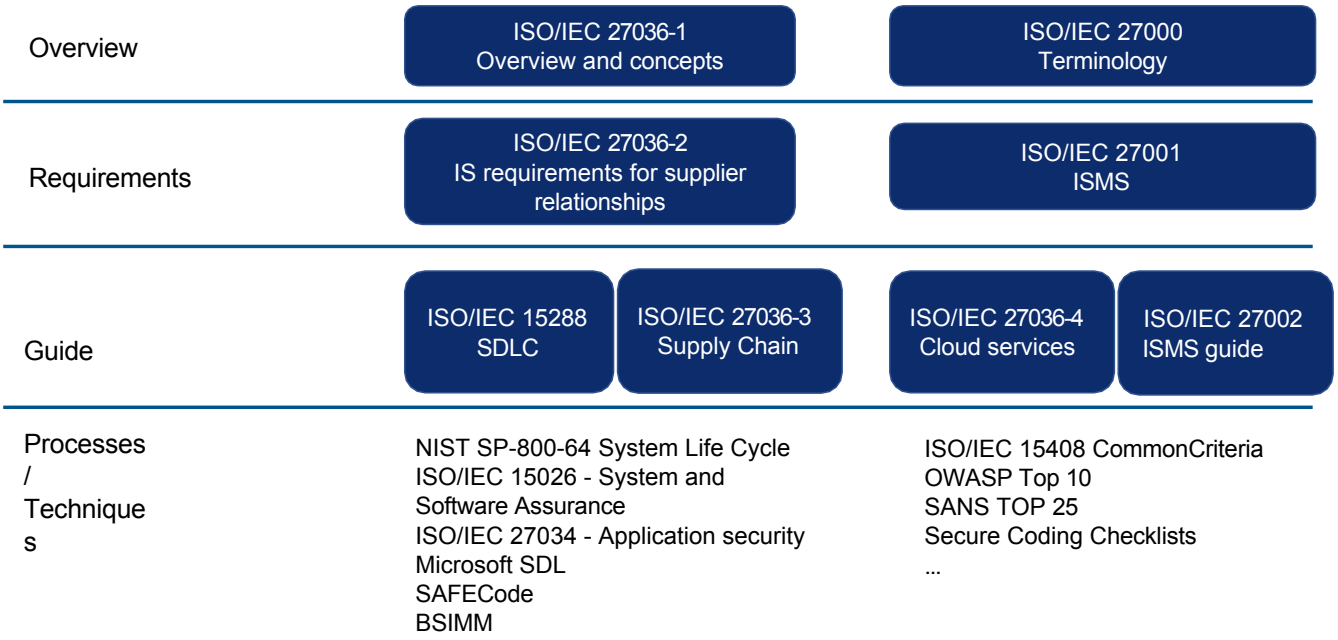


Figure 8: IS standards overview on supplier relationships

part of customer contracts. This standard also specifies requirements for information security (e.g., physical security, personnel security, IT security).

Success factors from practice

Holistic risk assessment

It is important to address all risks to which the own organization is exposed through cooperation with external service providers. At this point, the standard requires that all outsourced processes are clearly defined and sustainably controlled (see section 8.1).

One possible classification of supplier relationships is provided by ISO/IEC 27036-1, which distinguishes between:

- Supplier relationships for products
- Supplier relationships for services
- Information technology supply chain
- Cloud computing

Software use

The use of software of any kind should also be assessed under the aspect of supplier management. Both self-developed software and finished products and services often include frameworks, packages or other libraries. In the past, attacks on these components behind the actual application have led to successful compromises. Procedures for identifying and controlling these Components should be part of IT operations or software development.

Right to audit

The right to audit should be included in every contract.

- However, this right is not usually granted in standard contracts with cloud providers. In this
  In this case, alternatives must be examined, such as the inclusion of results reports from external audits or the provision of certificates including the respective areas of validity.

Certifications

Suppliers are increasingly responding to customers' demand for information security by means of certifications. ISO/IEC 27001:2022 or IT-Grundschutz are particularly suitable for this purpose. However, I S O / I E C 27018 for the processing of personal data in the cloud or - in part - the international standard ISAE 3402 "Assurance Reports on Controls at a Service Organiza- tion" are also used for this purpose. TISAX® has become established in the automotive sector. The basis for the test procedure is the VDA Information Security Assessment, which is based on ISO/IEC 27001.

- In all cases, a complete report on the au- dit and its results is very important, as the scope of a
  The audit and the controls audited in each case may vary. For critically classified suppliers, a SOC Type II report should be requested in accordance with ISAE 3402.

the. Furthermore, potential deviations should be evaluated by the client according to his own risk appetite.

- In the case of personal data, the use of service providers, in particular those that are outside the German legal area or outside the EEA[24] should be examined very critically.
- This context also includes the topic of commissioned data processing according to Art. 28 EU GDPR[25] independently. of where the service provider is located.

Key figures

The following key figures[26] can be used, for example, to evaluate information security in relation to service providers:

- Number of service provider reports delivered on time in relation to the total number of agreed reports
- Average time from detection to reporting of security incidents by service providers
- Number of service providers contractually assuring IS measures in relation to all service providers.
- Number of security incidents at service providers in the past reporting period

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Definition of the scope, taking into account the dependencies on external partners and service providers. leisters (section 4.3)

In addition, the following documents have established themselves in practice as target-oriented:

- Processes and procedures for service provider relationships (cf. ISO/IEC 27001:2022, sections 5.19-5.22). There shall-
  The requirements resulting from the procurement strategy and any service provider relationship should be defined. In addition, information security risks should be addressed within the ICT service and product supply chain.
- Agreements on information security requirements with suppliers. Here, the different
  categories of suppliers are taken into account.
- Topic-specific guideline for the use of cloud services (cf. ISO/IEC 27001:2022, section 5.23)
- Industry-specific safety requirements, such as the BDEW white paper from the energy sector

References

ISO/IEC 27001:2022 - Sections 4.3 and 8.1
and 5.19 - 5.23

ISO/IEC 27036-1:2021

BDEW white paper "Requirements for secure control and telecommunication systems".

3.12 Internal Audit

The primary objectives of internal ISMS audits are to check the extent to which the ISMS meets the organization's own requirements and the requirements of ISO/IEC 27001:2022 (compliance check) and to check the implementation and effectiveness of measures taken (implementation and effectiveness check).

For this purpose, an audit program must be planned and implemented that regulates aspects such as frequency, procedures, competencies and responsibilities, planning requirements, follow-up and reporting. Furthermore, it must be defined how corrective and preventive actions (i.e., actions directly derived from the audits) are handled and where they are "kept" for further processing.

The audit program is intended to ensure that all business processes covered by the ISMS (according to the scope) are audited at least once every three years with regard to the information security requirements and guidelines applicable at the time of the audit and with regard to conformity with the ISMS. Evidence of this must be provided.

Internal audits within the meaning of the standard do not refer to the activities of the internal audit function in the narrower sense, although this can also be a body that carries out internal audits. In practice, internal ISMS audits are a central task of the ISMS manager/CISO, who plans and manages audits - possibly together with an internal audit team or with the help of external support and taking ISO 19011:2018 into account.

Success factors from practice

Two areas can be distinguished in the implementation of internal audits (see Figure 9):

- The "audit program" or "audit framework," which serves as an organizational superstructure for controlling and

24 EEA: European Economic Area.

25 EU-DSGVO: EU General Data Protection Regulation.

26 See also: Assessing the performance of an ISMS using key indicators (ISACA Germany Chapter).

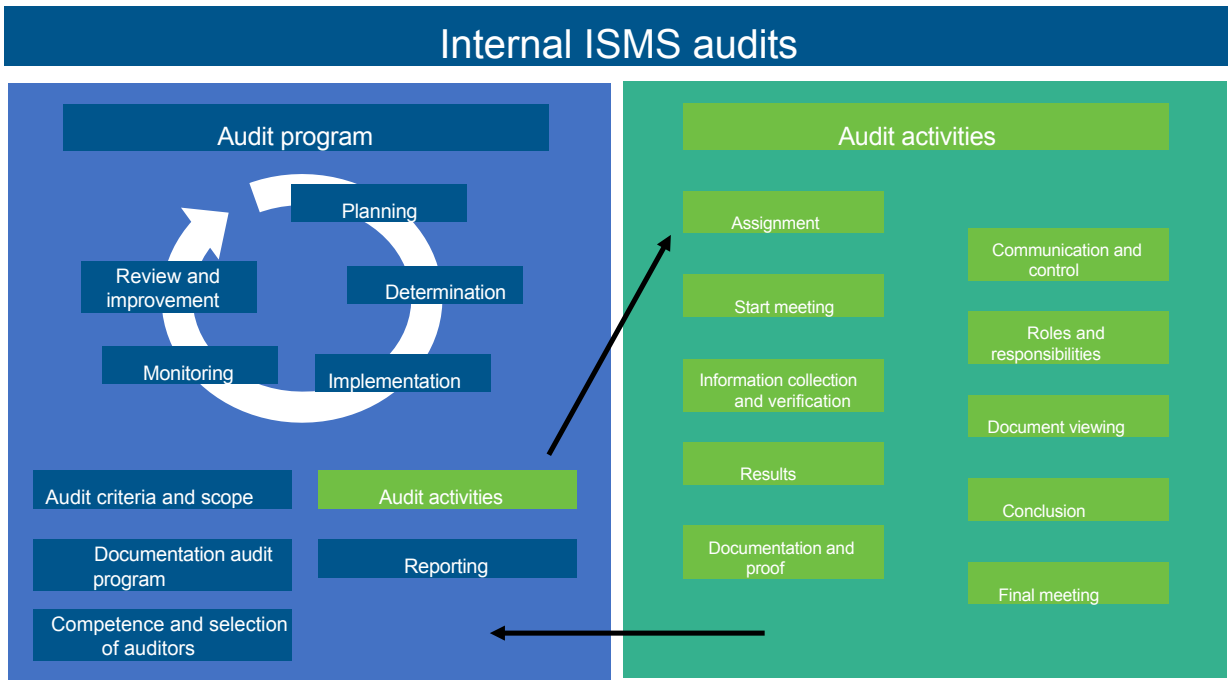


Figure 9: Structure for internal ISMS audits (audit program vs. audit activities)

The ISMS serves to monitor all activities in the context of internal au- dits and forms the interface to other processes in the ISMS.

- The specific "audit activities", which involve the planning and practical implementation of individual internal Audits include.

The audit activities serve the operational implementation of the audit program, so coordination with the organization's internal auditing function makes sense.

In larger organizations, it makes sense to divide these areas organizationally, with an audit team leader responsible for the audit program and a team of auditors carrying out the internal audits in practice. It must be ensured that both the overall design and the operational management of the audit program work optimally towards achieving the IS objectives. This gives the organization the best possible return on investment (ROI) for the resources used in the audit area.

The audit program

The audit program consists of a cycle with the sub-processes planning, definition, implementation, monitoring, and review and improvement of the audit program itself (see Figure 10).

- In the audit program and in the risk-based planning of specific audit activities, both the significance of the affected processes (core processes, damage impact, business criticality) and IT systems as well as the results of previous audits are taken into account.
- The audit program must define the general criteria for audits. Depending on the size of the organization, Depending on the number of audits performed and the desired level of detail of the audit program, the specific scope of individual audits can also be defined directly here.
- Audits that have been carried out must be documented and the corresponding information (e.g. in the form of audit The audit report must be available as proof of the implementation of the audit program.
- Regular management reports are to be prepared with information on the performance of the audit program and on the on the audit activities and their results.

Planning" sub-process

The audit program should be based on the individual requirements of the respective organization (see sections 4.2 and 4.3 of the standard and chapter *3.1 Context of the Orga- nization of* this guide). Furthermore, the defined objectives of the audit program should indicate that

- the audits are oriented to the risks identified,
- the importance of the individual business processes is taken into account and
- the audit program covers the scope of the associated ISMS.

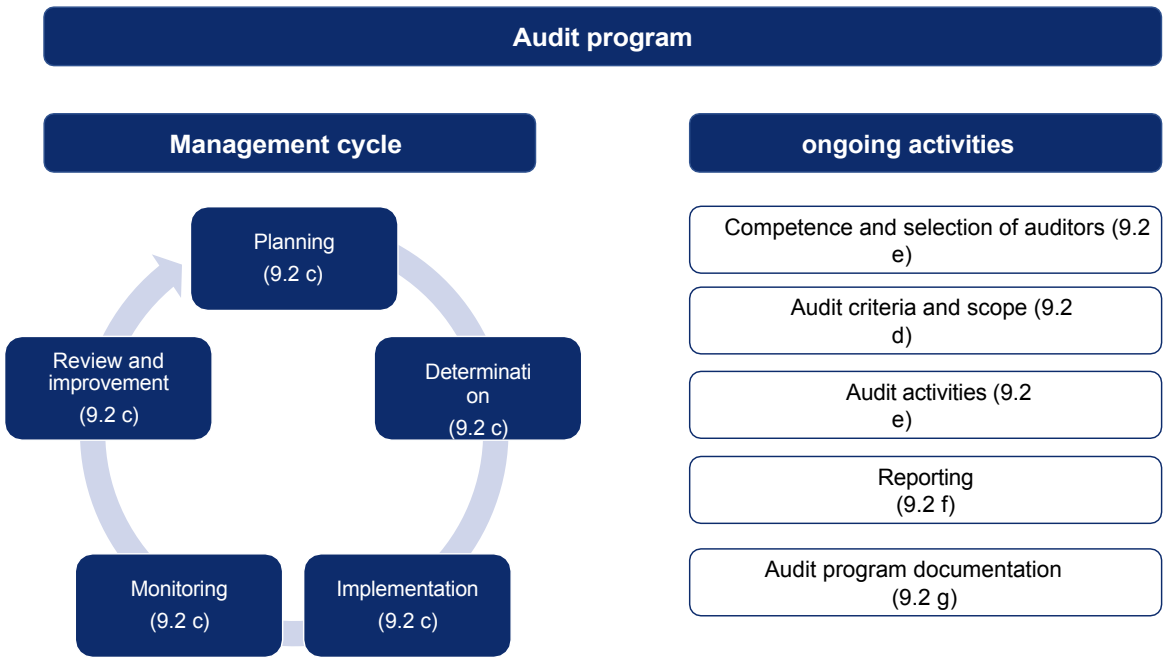


Figure 10 - Audit program [requirements27]

Sub-process "Determination

The employee responsible for the audit program must perform the following duties, among others:

- Definition and implementation of the entire audit program
- Identify, assess, and address risks directly impacting the audit program (e.g.,too scarce resources, gaps in auditor qualifications, areas of consideration too large for individual audits).
- Establishment of processes for the implementation of audits
- Determination and procurement of the necessary resources
- Determination of the audits and definition of the areas and criteria for the individual audits
- Determination of the methods and tools to be used
- Selection of auditors with ensuring their qualification and experience
- Ensure that audit program records are kept current at all times
- Ongoing monitoring and improvement of the audit program itself

Implementation" sub-process

For the implementation and execution of the audit program, the decisions made during the definition are to be implemented.

Whether objectives and the scope of individual audits are already defined here depends on the respective design or the level of detail of the audit program. The objectives and scope of audits generally result from the individual requirements and the protection needs of the IT systems concerned.

It is highly recommended to select the areas to be audited in such a way that they can be audited individually and with manageable effort. Further factors for the selection of the areas to be audited are the criticality of the business or service processes and the tolerable period between two audits. The total number of audited areas (within three years) must, of course, correspond to the scope of the ISMS.

Monitoring" sub-process

In the "monitoring" sub-process, the audit program itself must be continuously monitored with regard to quality and efficiency. Among other things, it must be questioned whether

- the audit program is still aligned with the scope of the ISMS and the business requirements,
- the time and resource planning are designed appropriately,

27 References in parentheses are to clause 9.2 of ISO/IEC 27001:2022.

- the "right" processes/areas/applications/systems/data are audited and
- the depth of testing as well as the type of testing are suitable to optimally support the objectives.

It is helpful to document the effort per audit. Since the effort required can vary depending on the characteristics of the IT system and/or the organizational unit concerned, data is collected in this way so that the effort required for future audits can be better estimated.

When monitoring the performance of the audit team members, it is important to pay attention to the quality, for example the objectivity, clarity and comprehensibility, of the audit results. Among other things, it is relevant here whether the department responsible for an IT system has received comprehensible, suitable and complete recommendations for action in response to identified deficiencies. If recommendations for action are not understood because, for example, information is missing or recommendations for action are not appropriate, this indicates that the members of the audit team need additional technical or methodological support.

This sub-process also includes the collection and evaluation of feedback from management, the audited areas or organizational units, the auditors and other stakeholders.

Review and improvement" sub-process

In the "Review and Improvement" sub-process, the persons responsible for t h e audit program regularly check whether the expectations of the stakeholders are still being met. The starting point is the information gathered in the subprocess "Monitoring" have been collected. Furthermore, the continuous professional and methodological development of the auditors must be determined and controlled.[28]

The status of the audit program must be reported to the responsible management. It is also useful to introduce KPIs to make the quality level of the audit program and the internal audits as a whole measurable and comparable. Quality statements such as "Proportion of measures accepted by departments and initiated for implementation" are more important than purely time-based statements such as "Quality of the internal audit program" or "Quality of the internal audit".
z. e.g. "working time spent per audit" to be preferred.

Competence and selection of auditors

- ISMS auditors should be selected to ensure the necessary objectivity, expertise and impartiality.
  The auditors are responsible for ensuring the quality and reliability of the audit process.
- The necessary competencies of an internal auditor should be described (e.g. in a role or position description).
  len description).

Planning and execution of audits

Audits are used to identify both non-conformities to existing specifications and potential previously unknown weaknesses and hazards.

- When it comes to audit planning, the following applies: no audit without a dedicated audit assignment. This means that the actual work is
  The audit should not begin until the assignment has been secured and formally communicated. In addition, the area to be audited should be actively involved in audit planning, for example, to coordinate the scope (what will be audited against), scheduling and the availability of contact persons during the audit.
- If possible, (immediate) measures for the appropriate treatment of hazards should already be taken in the audit.
  to be derived. However, implementation must be formally coordinated with t h e respective service, system and/or risk owners.
- If previously unknown deficiencies or risks inherent in the process are identified, the treatment of which in the short term is
  is not possible, these are to be included in the central risk inventory.
- Audit results must be regularly reported to the ISMS management level (at least in consolidated form).
  be
- Audit reports must clearly state which systems and documents have been audited or reviewed and used as the basis for the audit.
  were used for the audits.
- Open communication that is maintained throughout the entire duration of an audit makes a significant contribution to
  This helps to reduce reservations on the part of the audited area and thus lowers the risk that information is withheld or not presented in a realistic manner.[29]
- To determine the suitability, completeness and effectiveness of the implemented measures, the re
  In the course of the audit, the auditor directly questions the employees primarily responsible for the operation and monitoring of these measures, examines the documentation and/or arranges and assesses practical demonstrations. The auditors are required to have extensive technical knowledge and methodological skills. It is therefore appropriate to select the auditors on the basis of the objectives and contents of the audit in question.

28 See also section 7 of ISO/IEC 19011:2018.

29 See also "Communication - The Missing Piece," ISACA Journal 3/2012 *(https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/archi-*

- In the context of planning individual audits, i.e. before the start of implementation, the responsible lei-
  The assumption of the costs incurred must be clarified at all levels of management.

- At the latest in the final meeting of an audit, the results are to be reviewed together with the audited area.
  The audit report should be formally accepted by the auditor, who should understand and accept the findings and recommendations for action. Formal acceptance of the audit report should be sought. Disagreements that cannot be resolved should be documented in the report.

- Ensure that relevant information and audit reports are kept confidential and protected from unauthorized access.
  The data must be stored and archived in such a way that it is protected from unauthorized access.

- The requirements from section 9.2 for internal audits can be met by implementing the recommendations from Section 6.4 of ISO/IEC 19011:2018 and ISO/IEC 27007:2020 (see Chapter 8.5 *Implementation of internal ISMS audits (process diagram)*, page 62), although it should be noted that the normative requirements of ISO/IEC 27001:2022 are by no means as extensive as those described in current best practices.

- Further information on internal audits can be found, for example, in ISACA's QAR IT Guide. This guide is geared towards internal IT auditing, but can also be applied mutatis mutandis to internal ISMS audits.[30]

Differentiation of internal ISMS audits from certification audits

Internal (ISMS) audits are an essential instrument in the continuous improvement process of the management system. They are used to check whether the management system meets the organization's own requirements and where there is potential for improvement. The audit program ensures that all areas of the scope are effectively controlled by the management system.

Certification audits are always external audits. They are performed by qualified external auditors on behalf of a certification body. External auditors usually work on the basis of the two standards ISO/IEC 27006:2015 "Requirements for bodies providing audit and certification of information security management systems" and ISO/IEC 17021-1:2015 "Conformity assessment - Requirements for bodies providing audit and certification of management systems".

Differentiation of internal ISMS audits from the internal control system (ICS)

A company's internal control system (ICS) represents an essential 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 also includes, above all, specialist process controls.

In an ICS, a distinction is made between process-integrated and process-independent control activities. The former are usually control measures that result from risk analysis, good management practices or internal and external requirements (e.g. dual control principle for booking approval, multifactor authentication for critical users, etc.) and can therefore have the recommendations of ISO/IEC 2700x as their origin. This is the so-called "first line of distribution", which is intended to ensure the regularity of processes and activities in the company and is performed by the direct management level.

The effectiveness of the control measures can also be checked independently of the process, for example by an ISMS outside IT or by a compliance function. In practice, this is often referred to as the "second line of defense". This review does not replace the activities of the internal audit department, which in turn should review the effectiveness of the entire ICS as the so-called "third line of defense".

- If an ICS has already been established or is in the process of being established or changed, it is worth checking whether
  and to what extent the control and audit requirements of the ISMS can be taken into account or even partially integrated there. Complete integration will not be possible in practice, as the objectives of the two systems differ substantially. However, organizational interfaces to the ICS and the internal audit are recommended in any case.

- In practice, COSO or COBIT, for example, are used to model an ICS.

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Documentation of the audit program(s) (section 9.2 g)
- Documentation of audit results (section 9.2 g)

30 *See https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_ii_2016_overall_screen.pdf.*

References

ISO/IEC 27001:2022 - Section 9.2

ISO/IEC 19011:2018

ISO/IEC 27006:2015

ISO/IEC 27007:2020

ISO/IEC 17021-1:2015

3.13 Incident Management

Although it is not explicitly mentioned in the normative part of the standard, the management of information security incidents is another elementary component of a well-functioning ISMS.

Security-relevant incidents are usually non-conformities which, if their causes are investigated, have a decisive influence on the continuous improvement process (CIP) and the maturity of the ISMS. After all, only those who recognize errors and learn from them, i.e., who rethink their activities and strategies and, for example, remove or replace ineffective measures, adapt existing (security) concepts or implement new (security) measures, will also obtain the best possible long-term benefit from a management system operated within "unpredictable" framework conditions (= risks).

Success factors from practice

In order to maintain information security in operations, it is essential to anticipate the handling of information security incidents in the best possible way,
i.e. define responsibilities, procedures and treatment options in advance and also practice them.

The fundamental goal of the information security incident handling process is to ensure largely coordinated, targeted and thus efficient action when an actual security breach or targeted cyberattack occurs (see Figure 11).

- In this chapter, "only" the topic of "information security incidents" is addressed. For the development of a holistic emergency preparedness system, reference is made to ISO 22301:2019 "Security and resilience - Business continuity management systems - Requirements".
- The organization must define a categorization for incidents that makes sense for itself and that allows for a practicable and reasonable delineation of severity, for example, distinguishing between incidents, safety incidents, emergencies, and crises.
- An Incident Response Plan should be developed that identifies the key issues to be addressed. processes are defined (see ISO/IEC 27001:2022, Annex 5.24). Although this cannot cover every eventuality, it serves as a guide when an incident occurs and ensures a targeted approach.
- In an emergency, only what has already been communicated and practiced several times will work. Who instead of If you rely on the fact that the employees concerned (who are they?) still know "in the event of an incident" where they have to look in their treatment plan (where was it stored again?) in order to follow the instructions there immediately and appropriately, and that the managers responsible according to the plan also know what to do with the information flowing into them, you will b e only slightly better prepared than someone "without a plan" when a real security incident occurs - at least for the first few minutes or hours. However, "in the event of an incident," that's exactly what m a t t e r s . Therefore, it is not enough to have the plan in the drawer - it must be known and the procedure must be trained.
- The security incident handling process and its level of detail should be tailored to the risk appetite of the organi sation and the framework conditions of the ISMS.

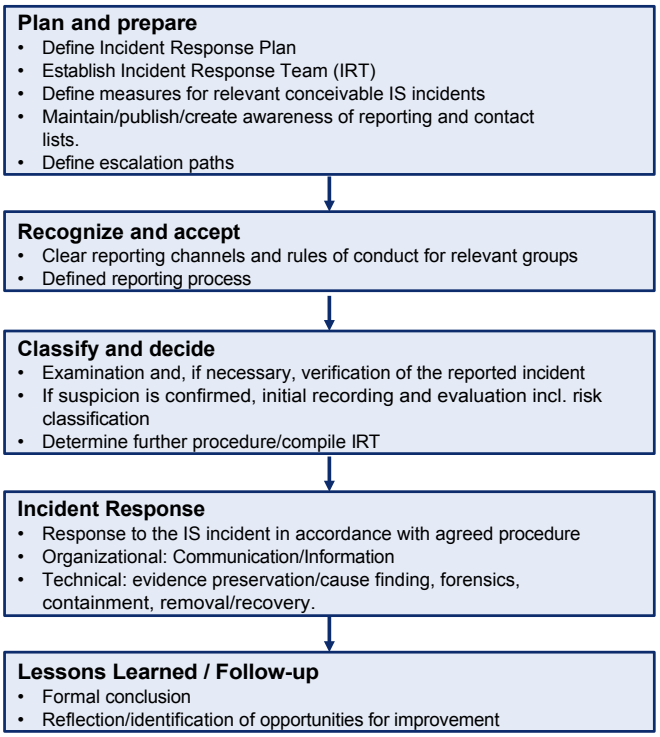


Figure 11: Incident Response Management - Phase Model b a s e d on ISO/IEC 27035-1:2023

Plan and prepare

In order to achieve the fundamental objective of the process, preventive measures must be taken for all operational phases of the process to prepare the organization and the employees for such an eventuality in the best possible way. In addition to generic problem-solving strategies, contact persons and escalation paths must be defined in advance.

Recognize and accept

- Security incidents should always be received at a central reporting point (irrespective of the time of receipt). All
  A clear reporting channel must be offered to relevant groups where IS incidents may occur, such as employees, IT suppliers, customers, and partners.
- Rules of conduct in the event of safety-relevant irregularities, including points of contact/reporting plans, should be target- oriented.
  be provided in a targeted manner.

Classify and decide

- The reporting office decides whether the reported event actually constitutes a safety event or whether it is
  an event that is not related to safety, a so-called "safety incident".
  "Known Error" ("Problem"), for which a solution description is already available, or even an emergency for which an emergency plan may exist. In case of doubt, escalation must take place here (if necessary via a "Manager on Duty"). The reporting office must be trained accordingly.
- All incoming incident reports should be documented. At a minimum, the following in-
  formations are recorded:
  - Unique identification number
  - Date of acceptance and entry of the Security Inci- dent
  - Name(s) of the reporter(s), name(s) of the person(s) concerned and identification(s) of the informatio- n/IT systems
  - Description of the security incident (How did the attacker proceed, which vulnerabilities were exploited? Damage caused so far)
  - Immediate measures already taken, if applicable
- All security incidents must be classified according to a predefined classification scheme (initial).
  so that a priority can be derived. Depending on the priority, predefined immediate measures must be initiated and the responsible persons (e.g., information security officer, CISO) informed.
- The security incidents documented in the (ticket) system should be subject to monitoring, if necessary, so that
  it is ensured that also low classified events are processed.

Incident Response

With regard to incident response, the following procedure has proven effective in practice:

1. **Containment and (initial) preservation of evidence:** Analysis of the extent and containment of the security incident as well as (initial) preservation of potential indications and evidence, if necessary by means of forensic analyses and predefined and practiced (!) procedures (see also Control 5.28).

   Examples of local mitigation measures:
   - Blocking compromised user accounts
   - Shutdown of attacked or compromised services
   - Use of malware tools (virus scanners, anti-spyware or similar programs) to clean systems superficially
   - Examples in the network:
     - Isolate compromised systems from the rest of the network and restrict access to a quarantine network.
     - Blocking of certain services and/or protocols and selected IP addresses
2. **Elimination and restoration:** Measures to restore the target state of an information/IT system: In many cases, this can be done by restoring the backup. In this case, the data and software are restored from "clean" backup files to "new" systems, whereby care must be taken to ensure that all vulnerabilities (which may still be present in the backup) are closed (if necessary, uploads and patches must be applied) and that the backup files are free of changes made by an attacker.

   Another measure may be, for example, updating system software and hardening the affected systems.
3. Root **cause identification and (extended) preservation of evidence**: Determination of the root cause of the event and preservation of potential clues and evidence, if necessary through further forensic analyses.

Lessons Learned/Follow-up

- The traceability of a security incident should be ensured at all times. This means that for each
  incident must be evident,
  - what the current status of the processing is (e.g. New, Accepted, In progress, Stopped, Solved, Closed),

  - who are the employees in charge of the processing, if any,
  - which measures are (currently) planned to solve the problem,
  - when the implementation of the required measures is planned.

- All documented safety incidents must (after processing) be subjected to an examination as to whether by Optimization of the Incident Response Plan or changes to the organizational structure and processes (including the creation or adaptation of instructions for action) can improve the handling of similar incidents in the future.

- When processing security incidents, it must always be documented at the conclusion how such incidents are to be avoided in the future or their impact is to be minimized. If necessary, further measures can be derived from this, which are to be transferred to regular operation.

Documentation requirements

According to ISO/IEC 27001:2022, there are no minimum documentation requirements.

However, in practice, the following documents have established themselves as target-leading:

- Incident Response Plan (IRP), including current (!) contact lists and escalation plans.

- Rules of conduct in the event of safety-related irregularities

- Process descriptions and work instructions for securing evidence

- IS Incident Reports

References

ISO/IEC 27001:2022 - clauses 5.24 - 5.28 and 6.8

ISO/IEC 27035-1:2023

ISO/IEC 27035-2:2023

ISO 22301:2019

3.14 Continual Improvement

Regardless of how many guides and books are available on the subject.
The reason why "optimal" management systems are not written is that they will probably never exist in practice, since organizations are too different to be able to manage them with a uniform management system.
"recipe" to serve. In addition, the general conditions are constantly changing, so there can never be a "best solution forever".

Organizations are therefore called upon to analyze existing best practices and apply them in a manner that is constantly adapted to their needs. In particular, they are called upon to derive improvement potential from their non-conformities and thus continuously improve their ISMS. This process is called continuous improvement process (CIP).

An organization that wants to operate a standard-compliant ISMS must therefore define organizational measures on the basis of which continuous improvement takes place in a targeted and planned manner. The implementation of these measures and the respective results must be monitored and appropriately documented. In addition, the organization must demonstrate how it ensures that any deficiencies identified are not repeated.

PDCA (Plan-Do-Check-Act) cycle

The recommended approach to sustainably ensure the continuous improvement of the ISMS can still follow the PDCA cycle, which is the basis of many management systems.

- **Plan**
  - Establishment of IS goals and responsibilities for their achievement
  - Establishment of the security measures to achieve the IS goals and the operational process responsible for these measures.
  - Define the performance indicators that allow performance measurement against the IS targets and associated monitoring measures.
  - Definition of the process for measuring the power including the measuring points, calculation method of the in- dicator and the standard and tolerance ranges.
  - Definition of corrective measures to regulate the safety measure in the standard range.

- **Do**
  - Continuous measurement of IS target achievement
  - Initiation of corrective actions in case of detected defects or non-conformities

- **Check**
  - Monitoring of the individual safety measures in indicators and comparisons of the individual performance capabilities with the IS targets.
  - Monitoring of the measures introduced with regard to implementation and their effectiveness.
  - Create security reports with key performance indicators for management based on IS objectives. These reports should include action options for necessary management decisions to strengthen security measures that regularly run into the tolerance range or exceed the threshold for ineffectiveness.

- **Act**
  - Making necessary management decisions
    gen to restore the effectiveness of safety measures. Decisions are passed on to operations for implementation.
  - The decisions made are appropriately documented with reasons, for example via security controlling.

Success factors from practice

The ISMS is usually improved by identifying deviations from the requirements and the corrective measures derived from them. However, it is also conceivable that suggestions for improvement are evaluated and implemented directly, i.e. without a deviation being present.

Possible sources of deviations and suggestions for improvement

- Conclusions from KPIs - analyses and measurements
- Follow-up of security incidents
- Results of (internal) audits
- Management review and control by the management
- Company suggestion scheme (suggestion for improvement)
- Measures derived from risk treatment
- Measures from the CIP should be included in an overarching implementation plan, so that an
  central consolidated or at least a business-area-wide list of measures exists.
- Furthermore, the regular risk analyses lead to a continuous improvement of the ISMS.
  The results of the risk treatment are an important part of the improvement of the ISMS, as risk-minimizing measures are identified and included in risk treatment plans for implementation.
- The overarching implementation plan facilitates monitoring on the implementation status and due date of implementa-
  The aim of the project is to ensure that the measures are implemented by the end o f t h e y e a r .
- Corrective action vs. corrective action: when deficiencies and nonconformities are identified, the organization must
  and correct or stop them (see sections 10.1 a and b). Corrections are used to rectify or eliminate non-compliant situations. In order to prevent the recurrence of the same error, it is necessary to conduct a sustainable root cause analysis and to define corrective actions (see sections 10.1 c to g).

Documentation requirements

According to ISO/IEC 27001:2022, the following minimum documentation requirements exist:

- Evidence on the nature of non-conformities as well as on implemented measures (section 10.1 f)
- Evidence of the effectiveness of a measure implementation (section 10.1 d)
- Evidence of results on all corrective actions (Section 10.1 g).

In addition, the following documents have proven to be useful in practice:

- Procedures for corrective actions (from section 10.1 c)
- Description of incident management and tracking of corrective actions
- Documentation tool for tracking the implementation status and verifying the effectiveness of
  Measures

References

ISO/IEC 27001:2022 - Section 10

ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2021 - Annex SL

4 Integration and operationalization of management systems

Integration of existing management systems

The previous guideline focuses on the implementation of an ISMS, but only marginally considers the integration of the management system into existing governance structures, which is often useful in this context, together with the associated opportunities and challenges, such as the use of synergy effects by bundling measures or control sets.

In practice, it is usually not possible, or rather not necessary, to introduce an ISMS in isolation as an island. In addition to other management systems already established in the organization, including their measures and processes, other operational or organizational circumstances must also be taken into account.

All management systems have large overlaps in structure, internal and external requirements, and thus also opportunities to use synergies. By harmonizing the requirements of the management systems, individual measures can be implemented across management systems, such as document control or the integrative use of risk assessments. This reduces the effort and risk involved in introducing, operating and verifying the management system.[1]

In this chapter, some of the challenges frequently encountered in companies and the associated approaches are outlined. It explicitly addresses not only new management systems to be introduced, but also potential improvements for established systems. Due to the immense increase in cyber security threats in recent years and the rapidly growing compliance requirements, especially for internationally active organizations, established systems must also ask themselves whether the current regulations/processes are still up to date in order to meet the growing tasks not only effectively but also efficiently.

Inquiries of the following type are now commonplace in ISMS departments:

- Please check if we are compliant with "China's Cyber Security Law".
- Which security measures are relevant for OT security?[2]
- A stakeholder/major customer would like a safety self-assessment according to ISO/NIST/BSI/VDA-ISA/EU-Have DSGVO carried out.

A new challenge is therefore the need to respond promptly to a growing number of compliance requirements, which often involve essentially the same or at least similar measures as the standards we are familiar with.

As a result - as a kind of bow wave of compliance requirement lists - mapping tables are also growing in which the respective controls, benchmarks, etc. are correlated with each other in order to be able to use already assessed implementations in other management systems, such as the ICS or the data protection management system.

In the meantime, some risk management/compliance/ISMS tool providers have adapted their solutions so that their own control objectives can be defined and linked to the control objectives of the various standards.

This makes it possible to check the degree of maturity or fulfillment of a standard at any time and to immediately recognize which con- troles of the selected standard still have open points or ri- sibilities.

1 See Annex SL.

2 See https://www.isaca.de/sites/*default/files/isaca_leitfaden_cyber-sicherheits-check_ot.pdf, page 17 ff.*

Operationalization through establishment of a "Corporate Control Database"

Based on the approach from the previous chapter, the introduction of a centrally maintained "corporate control database" represents an area of action in terms of continuous improvement of all existing management systems.

In most organizations, the managers responsible for a management system have currently still defined their own measures, which leads to the fact that many control measures, e.g. secure deletion of information, are maintained twice - if not three times - in different places in the organization, including all follow-up measures, such as e.g. ascertaining the implementation status, auditing, checking the effectiveness, etc. This undoubtedly leads to additional effort and, in particular, to a lack of understanding on the part of the person technically responsible for the subject. This inevitably leads to additional work and, in particular, to a lack of understanding on the part of those technically responsible for the topic, since the same questions are asked by various reviewers/auditors.

Those responsible are also affected by industry-, product- and service-specific norms, standards and best practices, which often conflict with each other. Meeting these requirements is made particularly difficult by a large number of different, manual and isolated processes.

The harmonized structure of management systems (according to Annex SL) has made many ISO management systems suitable for integration. Prominent examples are ISO/IEC 27001, ISO/IEC 27701, and ISO 22301. Other management systems not directly relevant to IT, such as quality management, occupational health and safety, and environmental protection, also follow the new structure and thus enable an organization-wide integrated management system in the context of GRC.

A corporate control database harmonizes rules across different specifications and guidelines for the user on the basis of a common framework. This is also accompanied by a changed approach in which the control measures are no longer aligned with standards but with topics. Alignment with domains (see below) is useful for this purpose.

The standards are assigned and maintained with the help of a meta-level. This meta-level thus enables measures that are consolidated for the entire organization[3]. This has the advantage that the answers to other "standards/laws/best practices" not previously considered become apparent, even if one has never previously been involved with the new compliance requirements. At the same time, this enables users to compile the requirements on an individualized basis in terms of industry, product and performance, and to monitor compliance with them.

In addition, they contain corresponding workflows and interfaces so that changes can be integrated automatically. In this way, governance requirements are consolidated and integrated into a holistic risk and compliance management system. The quality of the database grows with each new evaluation of a standard or norm.

Operationalization through alignment of "Central Corporate Controls" with domains

In practice, it has proven useful to group and align the aspects to be managed in the organization into domains in order to create a thematically clear assignment and responsibility. These domains should be integrated into the higher-level model of the organization in relation to its management systems, with COBIT being a suitable orientation.

Underlying domains from the area of information security could, for example, be taken from ISO/IEC 27002. With the new version, for example, grouping could take place according to the new property "Cybersecurity Con- cepts". Alternatively, grouping according to the BSI IT-Grundschutz-Kompendium or NIST Special Publication 800-53 would be conceivable. It is important that all areas in focus are covered.

The choice of control frameworks is of secondary importance and should be selected appropriately by the organization for its purposes, which may ultimately also vary due to external requirements or the business model. An automotive manufacturer is more likely to use TISAX, while the Cloud Security Alliance's (CSA) Cloud Control Matrix (CCM) is more suitable for a SaaS provider, for example, whereas the BSI Compendium will be primarily useful in the regulatory environment.

Whatever the organization decides, with appropriate software support or manual diligence, the ultimately selected standard can be maintained via a meta-level, so that many standards can be taken into account to a large extent. In this approach, the domain manager is responsible for resolving innovations, requirement conflicts or ambiguities at a central point. The quality of the database thus grows increasingly with each new evaluation of a standard or norm.

3 See, for example, the controls from the standards IDW PS 951, EU-DSGVO (ISO/IEC 27701:2019), ISMS (ISO/IEC 27002:2022), BCMS (ISO 22301:2019), QMS (ISO 9001:2015) to IT/OT Operations Controls.

5 Glossary

ADV Commissioned data processing - the processing of personal data by service providers (externally or internally by legally independent entities of a group of companies) in accordance with Art. 28 EU-DSGVO.

APT Advanced Persistent Threat

Asset Anything that has value to the organization, also called an infor- mation asset or information asset. There are many asset types, such as: Information, software, hardware, services, people and their qualifications, skills and experience, and intangible assets such as re- putation and image. ISO/IEC 27005:2022 distinguishes between primary and secondary assets, where pri- mary assets include business processes and business activities as well as information. Secondary assets support the primary assets, such as facilities, rooms, hardware, software, network, personnel, and websites.

BCMS Business Continuity Management System

BCS Business Criticality Scorecard

BDEW German Association of Energy and Water Industries

BIA Business Impact Analysis

BO Operating organization

BSI Federal Office for Information Security

BSIMM Building Security in Maturity Model

CCM Cloud Control Matrix

CERT Computer Emergency Response Team

CIO Chief Information Officer

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 with a focus on IT processes and control objectives.

COSO Committee of Sponsoring Organizations of the Treadway Commission - a U.S. organization that, among other things, developed the recognized standard for internal controls known as the COSO model.

CSA Cloud Security Alliance

DPO Data Protection Officer

DSGVO see EU-DSGVO

EU European Union

EU-DSGVO EU General Data Protection Regulation

EEA European Economic Area

GRC Governance, Risk and Compliance

ICT Information and Communications Technology

IEC International Electrotechnical Commission - an international standardization organization which, among other things, developed the ISO/IEC 2700x standard together with ISO.

ICS Internal Control System

IRP Incident Response Plan

IRT Incident Response Team

IS Information Security

ISA Information Security Assessments

ISAE International Standard on Assurance Engagements

ISB Information Security Officer

ISMS Information Security Management System - Part of the overarching management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. The management system includes the organizational structure, poli- cies, 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, synonymous with ISB

KCI Key Control Indicator

KPI Key performance indicator - a performance indicator

KRI Key Risk Indicator

CIP Continuous improvement process

MaRisk Minimum Requirements for Risk Management - an administrative instruction on the design of risk management in German credit institutions from the German Financial Supervisory Authority (BaFin)

NIST National Institute of Standards and Technology

NPS (Net Promoter Score) Indicator that measures the extent to which consumers would recommend a product or service to others.

OT Operational Technology

OWASP Open Web Application Security Project

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

QAR-IT ISACA Guide to Conducting a Quality As- surance Review of Internal IT Auditing (QAR-IT)

QMB Quality Management Representative

QMS Quality Management System

QA Quality assurance

RACI matrix Organizations use the categorization according to RACI to describe which role is responsible for which activities and which roles are to be involved. In this way, a clear description of responsibilities and competencies can be achieved. The terms are interpreted as follows:

- *Responsible* - responsible for the actual implementation (implementation responsibility). The person who takes the initiative
  for the implementation to others. Also interpreted as responsibility in the disciplinary and qualitative sense.
- *Accountable* - accountable (overall responsibility), responsible in the sense of "approve", "bil-
  ligen" or "sign". The person who bears responsibility in the legal or commercial sense. Also interpreted as responsibility from a cost center perspective.
- *Consulted* - consulted (professional expertise). A person whose advice should or must be sought. Also referred to as
  Responsibility interpreted from a professional point of view.
- to *be* Informed - *to be* informed (right to information). A person who receives information about the course or the
  The person receives the result of the activity or h a s the right to receive information.

As a rule, only one person (role) should *be accountable* per activity. However, several people can be *responsible*, *consulted* or *informed for an* activity. It is also possible that one person is *accountable* and *responsible for* an activity at the same time.

Risk Effect of uncertainty on objectives (definition according to ISO 31000:2018)

RPO Recovery Point Objective

RTO Recovery Time Objective

SaaS Software as a Service

Scope **Scope**

SDLC Software Development Life Cycle

SIRP Security Incident Response Process

SLA Service Level Agreement - Agreement between customer and service provider

SMART Specific, measurable, accepted, realistic, scheduled

SoA Statement of Applicability - documented statement of relevant and applicable control objectives and measures in the organization's ISMS.

SoD Matrix Segregation-of-Duties Matrix - Overview of functional segregations to be considered between roles within the organization.

TISAX Trusted Information Security Assessment Exchange

TMG Telemedia Act

UWG Unfair Competition Act

VDA Association of the Automotive Industry e.V.

Zero-day vulnerability A previously undisclosed and uncorrected vulnerability that could be exploited to manipulate or attack computer applications, data, or other network services.

6 References

Norms and standards

ISO 9001:2015 Quality management systems - Requirements

ISO 19011:2018 Guidelines for auditing management systems

ISO 22301:2019 Security and resilience - Business continuity management systems - Requirements

ISO 31000:2018 Risk management - Guidelines

IEC 31010:2018 Risk management - Risk assessment techniques

ISO Guide 73:2009 Risk management - Vocabulary

ISO/IEC 17021-1:2015 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 1: Requirements

ISO/IEC 17021-2:2016 Conformity assessment - Requirements for bodies providing audit and certification of management systems - Part 2: Competence requirements for auditing and certification of environmental management systems

ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements

ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls

ISO/IEC 27003:2017 Information technology - Security techniques - Information security management system - Guidance

ISO/IEC 27004:2016 Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation

ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection - Guidance on managing information security risks

ISO/IEC 27006:2015 Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007:2020 Information security, cybersecurity, and privacy protection - Guidelines for information security management systems auditing

ISO/IEC 27014:2020 Information security, cybersecurity, and privacy protection - Governance of information security

ISO/IEC 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018:2019 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 cybersecurity

ISO/IEC 27035-1:2023 Information technology - Information security incident management - Part 1: Principles and process

ISO/IEC 27035-2:2023 Information technology - Information security incident management - Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27036-1:2021 Cybersecurity - Supplier relationships - Part 1: Overview and concepts

ISO/IEC 27036-2:2022 Cybersecurity - 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 - Procedure for the technical work - Procedures specific to ISO -, Annex SL, 2021

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

More sources

COBIT 2019 for Information Security, ISACA 2019

BDEW whitepaper, Requirements for secure control and telecommunication systems, version 2.0, May 2018

BSI Standard 200-2, IT-Grundschutz Procedure, Version 1.0, 2017

BSI Standard 200-3, Risk analysis based on IT-Grundschutz, Version 1.0, 2017

IT-Grundschutz-Kompendium 2022, BSI, 2022

Guideline Cyber Security Check, Version 2, BSI/ISACA, 2020

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

7 List of figures/tables

Images

Tables

8 Attachments

8.1 Mapping Annex ISO/IEC 27001:2022 vs. Annex ISO/IEC 27001:2013

The following table shows the consistency of the measures from ISO/IEC 27001:2022 with ISO/IEC 27001:2013.

Mapping: ISO/IEC 27001:2022 vs. ISO/IEC 27001:2013		
ISO/IEC 27001:2022		**ISO/IEC 27001:2013**
5	**Organizational controls**	
5.1	Policies for information security	A.5.1.1, A.5.1.2
5.2	Information security roles and responsibilities	A.6.1.1
5.3	Segregation of duties	A.6.1.2
5.4	Management responsibilities	A.7.2.1
5.5	Contact with authorities	A.6.1.3
5.6	Contact with special interest groups	A.6.1.4
5.7	Threat intelligence	New
5.8	Information security in project management	A.6.1.5, A.14.1.1
5.9	Inventory of information and other associated assets	A.8.1.1, A.8.1.2
5.10	Acceptable use of information and other associated assets	A.8.1.3, A.8.2.3
5.11	Return of assets	A.8.1.4
5.12	Classification of information	A.8.2.1
5.13	Labelling of information	A.8.2.2
5.14	Information transfer	A.13.2.1, A.13.2.2, A.13.2.3
5.15	Access control	A.9.1.1, A.9.1.2
5.16	Identity management	A.9.2.1
5.17	Authentication information	A.9.2.4, A.9.3.1, A.9.4.3
5.18	Access rights	A.9.2.2, A.9.2.5, A.9.2.6
5.19	Information security in supplier relationships	A.15.1.1
5.20	Addressing information security within supplier agreements	A.15.1.2
5.21	Managing information security in the ICT supply chain	A.15.1.3
5.22	Monitoring, review and change management of supplier services	A.15.2.1, A.15.2.2
5.23	Information security for use of cloud services	New
5.24	Information security incident management planning and preparation	A.16.1.1
5.25	Assessment and decision on information security events	A.16.1.4
5.26	Response to information security incidents	A.16.1.5
5.27	Learning from information security incidents	A.16.1.6
5.28	Collection of evidence	A.16.1.7
5.29	Information security during disruption	A.17.1.1, A.17.1.2, A.17.1.3
5.30	ICT readiness for business continuity	New
5.31	Identification of legal, statutory, regulatory, and contractual requirements	A.18.1.1, A.18.1.5

➡

5	Organizational controls (continued)	
5.32	Intellectual property rights	A.18.1.2
5.33	Protection of records	A.18.1.3
5.34	Privacy and protection of PII	A.18.1.4
5.35	Independent review of information security	A.18.2.1
5.36	Compliance with policies and standards for information security	A.18.2.2, A.18.2.3
5.37	Documented operating procedures	A.12.1.1
6	**People controls**	
6.1	Screening	A.7.1.1
6.2	Terms and conditions of employment	A.7.1.2
6.3	Information security awareness, education and training	A.7.2.2
6.4	Disciplinary process	A.7.2.3
6.5	Responsibilities after termination or change of employment	A.7.3.1
6.6	Confidentiality or non-disclosure agreements	A.13.2.4
6.7	Remote working	A.6.2.2
6.8	Information security event reporting	A.16.1.2, A.16.1.3
7	**Physical controls**	
7.1	Physical security perimeter	A.11.1.1
7.2	Physical entry controls	A.11.1.2, A.11.1.6
7.3	Securing offices, rooms and facilities	A.11.1.3
7.4	Physical security monitoring	New
7.5	Protecting against physical and environmental threats	A.11.1.4
7.6	Working in secure areas	A.11.1.5
7.7	Clear desk and clear screen	A.11.2.9
7.8	Equipment siting and protection	A.11.2.1
7.9	Security of assets off-premises	A.11.2.6
7.10	Storage media	A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5
7.11	Supporting utilities	A.11.2.2
7.12	Cabling security	A.11.2.3
7.13	Equipment maintenance	A.11.2.4
7.14	Secure disposal or re-use of equipment	A.11.2.7
8	**Technological controls**	
8.1	User endpoint devices	A.6.2.1, A.11.2.8
8.2	Privileged access rights	A.9.2.3
8.3	Information access restriction	A.9.4.1
8.4	Access to source code	A.9.4.5
8.5	Secure authentication	A.9.4.2
8.6	Capacity management	A.12.1.3
8.7	Protection against malware	A.12.2.1
8.8	Management of technical vulnerabilities	A.12.6.1, A.18.2.3
8.9	Configuration management	New
8.10	Information deletion	New

➡

8	Technological controls (continued)	
8.11	Data masking	New
8.12	Data leakage prevention	New
8.13	Information backup	A.12.3.1
8.14	Redundancy of information processing facilities	A.17.2.1
8.15	Logging	A.12.4.1, A.12.4.2, A.12.4.3
8.16	Monitoring activities	New
8.17	Clock synchronization	A.12.4.4
8.18	Use of privileged utility programs	A.9.4.4
8.19	Installation of software on operational systems	A.12.5.1, A.12.6.2
8.20	Network controls	A.13.1.1
8.21	Security of network services	A.13.1.2
8.22	Segregation in networks	A.13.1.3
8.23	Web filtering	New
8.24	Use of cryptography	A.10.1.1, A.10.1.2
8.25	Secure development lifecycle	A.14.2.1
8.26	Application security requirements	A.14.1.2, A.14.1.3
8.27	Secure system architecture and engineering principles	A.14.2.5
8.28	Secure coding	New
8.29	Security testing in development and acceptance	A.14.2.8, A.14.2.9
8.30	Outsourced development	A.14.2.7
8.31	Separation of development, test and production environments	A.12.1.4, A.14.2.6
8.32	Change management	A.12.1.2, A.14.2.2, A.14.2.3, A.14.2.4
8.33	Test information	A.14.3.1
8.34	Protection of information systems during audit and testing	A.12.7.1

The following table shows the consistency of the measures from ISO/IEC 27001:2013 with ISO/IEC 27001:2022.

Mapping: ISO/IEC 27001:2013 vs. ISO/IEC 27001:2022		
ISO/IEC 27001:2013		**ISO/IEC 27001:2022**
A.5	**Information security policies**	
A.5.1.1	Policies for information security	5.1
A.5.1.2	Review of the policies for information security	5.1
A.6	**Organization of information security**	
A.6.1.1	Information security roles and responsibilities	5.2
A.6.1.2	Segregation of duties	5.3
A.6.1.3	Contact with authorities	5.5
A.6.1.4	Contact with special interest groups	5.6
A.6.1.5	Information security in project management	5.8
A.6.2.1	Mobile device policy	8.1
A.6.2.2	Teleworking	6.7
A.7	**Human Resource Security**	
A.7.1.1	Screening	6.1
A.7.1.2	Terms And Conditions Of Employment	6.2
A.7.2.1	Management Responsibilities	5.4
A.7.2.2	Information Security Awareness, Education And Training	6.3
A.7.2.3	Disciplinary Process	6.4
A.7.3.1	Termination Or Change Of Employment Responsibilities	6.5
A.8	**Asset Management**	
A.8.1.1	Inventory of assets	5.9
A.8.1.2	Ownership of assets	5.9
A.8.1.3	Acceptable use of assets	5.10
A.8.1.4	Return of assets	5.11
A.8.2.1	Classification of information	5.12
A.8.2.2	Labelling of information	5.13
A.8.2.3	Handling of assets	5.10
A.8.3.1	Management of removable media	7.10
A.8.3.2	Disposal of media	7.10
A.8.3.3	Physical media transfer	7.10
A.9	**Access Control**	
A.9.1.1	Access Control Policy	5.15
A.9.1.2	Access To Networks And Network Services	5.15
A.9.2.1	User Registration And De-Registration	5.16
A.9.2.2	User Access Provisioning	5.18
A.9.2.3	Management Of Privileged Access Rights	8.2
A.9.2.4	Management Of Secret Authentication Information Of Users	5.17
A.9.2.5	Review Of User Access Rights	5.18
A.9.2.6	Removal Or Adjustment Of Access Rights	5.18

➡

A.9	Access Control (continued)	
A.9.3.1	Use Of Secret Authentication Information	5.17
A.9.4.1	Information Access Restriction	8.3
A.9.4.2	Secure Log-On Procedures	8.5
A.9.4.3	Password Management System	5.17
A.9.4.4	Use Of Privileged Utility Programs	8.18
A.9.4.5	Access Control To Program Source Code	8.4
A.10	**Cryptography**	
A.10.1.1	Policy On The Use Of Cryptographic Controls	8.24
A.10.1.2	Key Management	8.24
A.11	**Physical And Environmental Security**	
A.11.1.1	Physical Security Perimeter	7.1
A.11.1.2	Physical Entry Controls	7.2
A.11.1.3	Securing Offices, Rooms And Facilities	7.3
A.11.1.4	Protecting Against External And Environmental Threats	7.5
A.11.1.5	Working In Secure Areas	7.6
A.11.1.6	Delivery And Loading Areas	7.2
A.11.2.1	Equipment Siting And Protection	7.8
A.11.2.2	Supporting Utilities	7.11
A.11.2.3	Cabling security	7.12
A.11.2.4	Equipment Maintenance	7.13
A.11.2.5	Removal Of Assets	7.10
A.11.2.6	Security Of Equipment And Assets Off-Premises	7.9
A.11.2.7	Secure Disposal Or Re-Use Of Equipment	7.14
A.11.2.8	Unattended User Equipment	8.1
A.11.2.9	Clear Desk And Clear Screen Policy	7.7
A.12	**Operations Security**	
A.12.1.1	Documented operating procedures	5.37
A.12.1.2	Change management	8.32
A.12.1.3	Capacity management	8.6
A.12.1.4	Separation of development, testing and operational environments	8.31
A.12.2.1	Controls against malware	8.7
A.12.3.1	Information backup	8.13
A.12.4.1	Event logging	8.15
A.12.4.2	Protection of log information	8.15
A.12.4.3	Administrator and operator logs	8.15
A.12.4.4	Clock synchronization	8.17
A.12.5.1	Installation of software on operational systems	8.19
A.12.6.1	Management of technical vulnerabilities	8.8
A.12.6.2	Restrictions on software installation	8.19
A.12.7.1	Information systems audit controls	8.34

➡

A.13	**Communications Security**	
A.13.1.1	Network controls	8.20
A.13.1.2	Security of network services	8.21
A.13.1.3	Segregation in networks	8.22
A.13.2.1	Information transfer policies and procedures	5.14
A.13.2.2	Agreements on information transfer	5.14
A.13.2.3	Electronic messaging	5.14
A.13.2.4	Confidentiality or non-disclosure agreements	6.6
A.14	**System Acquisition, Development And Maintenance**	
A.14.1.1	Information Security Requirements Analysis And Specification	5.8
A.14.1.2	Securing Application Services On Public Networks	8.26
A.14.1.3	Protecting Application Services Transactions	8.26
A.14.2.1	Secure Development Policy	8.25
A.14.2.2	System Change Control Procedures	8.32
A.14.2.3	Technical Review Of Applications After Operating Platform Changes	8.32
A.14.2.4	Restrictions On Changes To Software Packages	8.32
A.14.2.5	Secure System Engineering Principles	8.27
A.14.2.6	Secure Development Environment	8.31
A.14.2.7	Outsourced Development	8.30
A.14.2.8	System Security Testing	8.29
A.14.2.9	System Acceptance Tests	8.29
A.14.3.1	Protection Of Test Data	8.33
A.15	**Supplier relationships**	
A.15.1.1	Information security policy for supplier relationships	5.19
A.15.1.2	Addressing security within supplier agreements	5.20
A.15.1.3	Information and communication technology supply chain	5.21
A.15.2.1	Monitoring and review of supplier services	5.22
A.15.2.2	Managing changes to supplier services	5.22
A.16	**Information Security Incident Management**	
A.16.1.1	Responsibilities And Procedures	5.24
A.16.1.2	Reporting Information Security Events	6.8
A.16.1.3	Reporting Information Security Weaknesses	6.8
A.16.1.4	Assessment Of And Decision On Information Security Events	5.25
A.16.1.5	Response To Information Security Incidents	5.26
A.16.1.6	Learning From Information Security Incidents	5.27
A.16.1.7	Collection Of Evidence	5.28
A.17	**Information Security Aspects Of Business Continuity Management**	
A.17.1.1	Planning Information Security Continuity	5.29
A.17.1.2	Implementing Information Security Continuity	5.29
A.17.1.3	Verify, Review And Evaluate Information Security Continuity	5.29
A.17.2.1	Availability Of Information Processing Facilities	8.14

➡

A.18	Compliance	
A.18.1.1	Identification of applicable legislation and contractual requirements	5.31
A.18.1.2	Intellectual Property Rights	5.32
A.18.1.3	Protection Of Records	5.33
A.18.1.4	Privacy And Protection Of Personally Identifiable Information	5.34
A.18.1.5	Regulation Of Cryptographic Controls	5.31
A.18.2.1	Independent Review Of Information Security	5.35
A.18.2.2	Compliance With Security Policies And Standards	5.36
A.18.2.3	Technical Compliance Review	5.36, 8.8

8.2 Version comparison ISO/IEC 27001/2:2022 vs. ISO/IEC 27001/2:2013

Below you will find a brief description of the main changes to the content of ISO/IEC 27001:2022 and ISO/IEC 27002:2022 compared to the previous versions from 2013.

ISO/IEC 27001:2022 vs. ISO/IEC 27001:2013

In October 2022, the third edition of ISO/IEC 27001 was published. Like other ISO/IEC standards that describe requirements for a management system (e.g., ISO 9001, ISO 14001, ISO 22301), the ISO/IEC 27001 follows a uniform structure, the so-called "*Harmonized Structure*" from Annex SL of the ISO/IEC Directives, Part 1. Since this structure has changed in 2021, the main chapters of ISO/IEC 27001:2022 have been adapted accordingly. This has resulted in the following changes in the main chapters[1]:

- The organization (Chapter 4 "*Context of the organization*") has now, in addition to defining relevant requirements of interested parties, it is also necessary to define which of these requirements are addressed within the framework of the ISMS (Section 4.2 c).
- Management of change (Chapter 6 "*Planning*") has been added to Section 6.2 "*Information security objectives and planning to achieve them*" to include the aspect that, in addition to the requirements for defining and implementing information security objectives, these must also be monitored. The chapter was further expanded with section 6.3 "*Planning of changes*" for the implementation of planned changes to the ISMS. The circumstances requiring a change to the ISMS may be planned or unplanned (as described in Section 6.1 "*Actions to address risks and opportunities*"), but the changes themselves must be planned.
- In chapter 8 "*Operation*", the new version adds that explicit criteria for the implementation of the processes from Chapter 6 "*Planning*" must be established and the implementation must be carried out in accordance with these criteria.
- In Chapter 9 "*Performance evaluation*", sections 9.2 "*Internal Audit*" and 9.3 "*Management Review*" are divided into further subsections, but their contents remain identical.
- Section 9.3 "*Management Review*" has been divided into three subsections. Here it was added that management reviews, the changes in the needs and expectations of interested parties that are necessary for the ISMS are relevant (section 9.3.2. "*Management review inputs,*" (*c*).
- Continuous Improvement: Chapter 10 has been reorganized so that the statement, suitability, appropriateness and effectiveness of the ISMS on an ongoing basis, precedes the nonconformity section, with the goal of encouraging improvement rather than corrective action.
- The new version of ISO/IEC 27001:2022 contains in essence a complete replacement of Annex A, which is reflects the controls of ISO/IEC 27002:2022. The only difference between the information in the annex of ISO/IEC 27001 and the controls from ISO/IEC 27002 lies in the wording of the requirements: The annex to ISO/IEC 27001:2022 uses the word "shall", which means that the controls are mandatory, whereas ISO/IEC 27002 uses the word "should", which means that the requirements are to be understood as recommendations.
- The controls listed in the annex still do not claim to be complete, and there may be additional measures may be required. Companies are also free, as before, to use the measures from other sources (e.g., NIST Cybersecurity Framework, BSI IT-Grundschutz, ISF Standard of Good Practice, etc.) to mitigate their information security risks. In this case, all that is required is an applicability statement that includes a mapping from the selected measures to the controls from the Annex of ISO/IEC 27001:2022, as well as the required rationale for the selection. This confirms that no requirements have been neglected that are actually applicable and necessary to mitigate existing risks (cf. ISO/IEC 27001:2022, clause 6.1.3. "*Information security risk treatment*," (b) and Note 2 of Section 6.1.3; (c) has been slightly modified to further clarify this aspect).

ISO/IEC 27002:2022 vs. ISO/IEC 27002:2013

In the new version of ISO/IEC 27002:2022, the change in **title** from "Information technology - Security techniques - Code of practice for information security controls" to "Information security, cybersecurity and privacy protection - Information security controls" is already noticeable. The term "Code of Practice" was removed to better reflect its purpose as a tone-setting reference for information security measures. In addition to the word "Information Security", the terms "Cyber Security" and "Privacy Protection" are emphasized. As a result, the new version explicitly addresses cyber security measures as a subset of information security measures and privacy protection measures.

1 In the following, the term "chapter" is also used for ISO/IEC 27001:2013.

The content of ISO/IEC 27002:2013 has been significantly expanded: The 2013 standard consists of a total of 80 pages (plus 10 pages of table of contents and foreword), whereas the updated version comprises 131 pages (plus 10 pages of table of contents and foreword as well as 17 pages of annex). The 2013 standard contains references to 27 other ISO standards, while the new version contains more than twice as many. In total, 56 other sources are referenced.

A chapter/glossary for terms, definitions and abbreviations has also been added, instead of an exclusive reference to ISO/IEC 27000, as was the case in the old version.

The structure of the new ISO/IEC 27002:2022 has been completely revised. As a thematic structure, the new version now contains 4 topics instead of 14 chapters/domains ("Security Control Clauses") (see below in more detail). Directly downstream of these are the 93 measures ("Controls"). Thus, the original integration into "Control objectives" is omitted for the time being. In the future, this will be presented as a purpose for each measure. All in all, measures in the new version comprise the following contents:

- a short description of the measure ("*Control title"*),
- additional attributes ("*Attribute table"*),
- a description of the control,
- a description of the purpose of the control ("*Purpose*"),
- an implementation guide for the control ("*Gui- dance"*) as well as
- explanatory text or references to other related documents ("*Other Information"*).

As mentioned above, measures in the new version are divided into 4 topics:

- ***"People controls,"*** chapter 6, for measures that focus on people, such as "screening" or "Remote working";
- ***"Physical controls"***, Chapter 7, when physical items are involved, such as access control;
- ***"Technological controls,"*** chapter 8, when technology is involved; and
- all other measures are assigned to ***"Organizational controls"***, chapter 5.

A helpful addition in the new version are the at- tributes ("*Attribute table"*), which can be assigned to five different categories:

- "Control types (possible values: preventive, detective, corrective),
- "Information security properties" (possible values: confidentiality, integrity, availability),
- "Cybersecurity concepts" (possible values: identify, protect, detect, respond, recover),
- "Operational capabilities (possible values: e.g. physical security, governance) and
- "Security domains" (possible values: e.g. protection, defence).

With the help of these new attributes, the focus on certain aspects can be set much better, e.g. different views can be created for different target groups, requirements can be categorized and the measures can be filtered easily.

The restructuring at the measure level has the following effect: In the new version, 11 new controls have been added, one control has been split, 57 controls have been merged into 24 controls, and 58 controls have been reworded.

The new version thus contains 93 measures/controls in 4 topics compared to 114 measures/controls in 14 Security Control Clauses in the old version.

New measures

As mentioned above, there are 11 new measures in the new standard:

- "*Threat intelligence*" (Section 5.7) is definitely new in this form. This involves, among other things, the collection and
  Evaluation of information on the specific threat environment of the organization in order to be able to take appropriate reactive measures: A distinction is made between strategic, tactical and operational threat intelligence.
- "*Information security for use of cloud services*" (sec. 5.23), this measure was not available in the 2013 version. implicitly anchored in supplier relationships. The measure covers the information security of cloud services from the customer's point of view. For example, a guideline on cloud computing in the company is required.
- "*ICT readiness for business continuity*" (section 5.30); ICT here stands for "Information and Communications Technologies" and the measure goes beyond the old information security aspects of business continuity management (old version, Clause 17): for example, the performance of business impact analyses (BIA) is described as a basis.

- *"Data masking*" (Section 8.11) deals not only with the topic of masking of (person-related)
  The study also discusses the properties of pseudonymization and anonymization of data, and addresses legal aspects.
- "*Data leakage prevention*" (Section 8.12) expands on the original requirement for information classifica-
  and offers a wide range of measures to protect against data leakage, including the aspects of monitoring and its technical implementation.

The other new measures are:

- "*Physical security monitoring*" (section 7.4)
- "*Configuration management*" (section 8.9)
- "*Information deletion*" (section 8.10)
- "*Monitoring activities*" (Section 8.16)
- "*Web filtering*" (Section 8.23)
- "*Secure coding*" (section 8.28)

Split measure

One measure has been split into two separate measures in the new standard:

The measure "*Technical compliance review*" (old version, Security Control Clause 18.2.3) is divided into two parts: firstly, the organizational part "*Compliance with policies and standards for information security*" (Section 5.36), with explanations of how to check compliance with the guidelines, and secondly, the technical part "*Management of technical vulnerabilities*" (Section 8.8), which has been greatly expanded and is described in detail. For example, the identification and evaluation of technical vulnerabilities is discussed in detail, and the performance of pentests is explicitly recommended.

Measures summarized

A total of 57 measures were combined into 24 measures, which represents a significant compression. At this point, we will limit ourselves to two selected examples:

- "*Information security in project management*" (Section 5.8) was developed from 2 original domains/security con-. trol Clauses have been merged. On the one hand, the content of the measure "*Information security in project management*" (old version, Security Control Clause 6.1.5), and on the other hand, the content of "*Information security requirements analysis and specification*" (old version, Security Control Clause 14.1.1) have been included.
- "*User endpoint devices*" (Section 8.1) was also created from 2 original Domains/Security Control Clauses to-. merged. On the one hand, the content of the measure "*Mobile device policy*" (old version, Security Control Clause 6.2.1), and on the other hand, the content of "*Unattended user equipment*" (old version, Security Control Clause 11.2.8) have been incorporated. This brings together all aspects that need to be taken into account in the protection of end user devices.

Evaluation

The new version represents a significant further development and an update with regard to recognized information security measures, as promised by the standard in its introduction. Important best practices and trends in the information security industry have been taken into account in the new version, although no massive thematic expansions have been made with 11 new measures.

The division into organizational, personal, physical and technical measures offers a significant improvement in the structure from the point of view of the authors. Compared to the 2013 version, extensive additional information is listed and more detailed help is provided. Texts and definitions have been sharpened and the attributes provide consistency in interpretation. The attributes of the *"Cybersecurity concepts"* category, for example, correspond to the functions of the NIST Cybersecurity Frame- work, thus creating a direct link to another management framework.

With these and other formal additions, a variety of views of different sub-aspects can be created. These options and the higher level of detail can simplify the creation of company-specific guidelines.

Outlook

The update of other existing standards and stan- dards of the ISO/IEC 27000 series, which have adopted the structure of ISO/ IEC 27002:2013, will follow and is expected to be completed by 2024.

Organizations already have the option of using the new measures from Annex A as measures. With the mapping tables available, declarations of applicability can also be created for certified companies, which still correspond to the previous 2013 version if required. With the publication of the ISO/IEC 27001:2022 version, this step should only be necessary for obtaining certification if certification is still to be carried out explicitly according to the 2013 version. This could be necessary, for example, if the certification body has not yet been accredited for certification according to the 2022 version.

has. The document "Transition Requirements for ISO/IEC 27001:2022" of the International Accreditation Forum[2] regulates the transition from version 2013 to version 2022. Existing measures of a certified ISMS can thus be adapted to the new ISO/IEC 27002:2022 and thus to the new annex within the framework of a three-year transition period (by 31.10.2025 at the latest). Due to the provided mappings, the effort for such an adaptation should essentially be able to focus on the new measures as well as on improvements of existing measures of the standard.

Certification bodies must begin certifying to the new standard no later than Oct. 31, 2023.

8.3 Holistic protection of the value chain

One of the central aspects of introducing or adapting the ISMS/cyber security strategy should be the introduction of a process for securing the value chain of the organization to be protected by the ISMS. This measure can be used to lay the foundation for end-to-end security management, which ensures basic protection throughout the entire company and determines further activities on the basis of risk.

In practice, a "Business Criticality Scorecard (BCS)" has become established for this purpose,

These are used, for example, to document a scenario-based classification of the basic risk level of the process or the applications used in it.

For end-to-end protection, it is useful that the organization assesses the criticality of the process and the need for protection of the information processed in it on the basis of a policy for at least each main process and for each application operated for the process by the respective process owner in such a scorecard.

In addition, it is important that an organization's project methodology ensures that such a scorecard is created for new projects (analogous to the data protection and/or works council notification) so that information security requirements can be coordinated at an early stage.

Scenario-based prioritization of the business processes to be protected

The scorecard for business criticality is used to perform a high-level identification of the information security risks resulting from the process or the applications in order to determine the effort required to protect the asset under consideration. Here, identification based on organization-specific fundamental questions and scenarios in the context of information security objectives, which are illustrated below as examples (see Figure 12), is a suitable approach.

Scenario: Imagine if a hacker (and/or a competitor) had access to the process data/information? **[Confidentiality]**	How do you assess the risk to OUR ORGANIZATION? W: Select an element. S: Select an element. Select an element. Risk level Describe the specific damage that has occurred to OUR ORGANIZATION. would be conceivable.
Scenario: Imagine that a hacker (and/or a competitor) could corrupt the service's data/information ("loss of integrity"). **[Integrity]**	How do you assess the risk to OUR ORGANIZATION? W: Select an element. S: Select an element. Select an element. Risk level Describe the specific damage that has occurred to OUR ORGANIZATION. would be conceivable.
Scenario: Imagine that the service or data would be unavailable for more than one day. **[Availability]**	How do you assess the risk to OUR ORGANIZATION? W: Select an element. S: Select an element. Select an element. Risk level Would there be a workaround to meet the business requirements (e.g. manual process)? At what point would a failure be critical to OUR ORGANIZATION? Select an element.

Figure 12: Scenario-based determination of the risk level

2 International Accreditation Forum, Inc, Transition Requirements for ISO/IEC 27001:2022, Issue 1 (IAF MD 26:2022).

In addition to the criticality and risk assessment, other facts can also be collected, e.g., on the RTO/RPO or on processes relevant to operations. A scorecard must include at least a description of the main process under consideration or the applications operated for it, as well as a unique identifier.

Based on the information collected, e.g., maturity level implementation of the baseline requirements and documentation requirements, and in particular based on the criticality and risk assessment collected, the information security officer (ISO) in BCS decides what effort needs to be invested in further security analysis (of the process) in order to achieve an adequate security level for the organization.

For less critical systems, for example, a standard safeguard to be defined can be applied, and for processes with higher risk potential, specific safety concepts or technical checks, such as
z. e.g., the performance of a penetration test. The possible decision stages could be defined as exemplified in Table 3.

Stage	Effort safety analysis
0	No further analysis necessary
1	**Standard measures** Performing a GAP analysis on the organization's standard measures or alternatively, if operated by the Group's own IT, confirmation from the IT department that the measures have been implemented.
2	**Advanced safety analysis** Conduct a specific vulnerability assessment using threat modeling (e.g., STRIDE[3]).
3	**Technical safety analysis** Performance of a penetration test or source code analysis by an independent third party

Table 3: Effort safety analysis

The BCS thus represents a kind of "pre-filter" for risk management, since extensive analyses can only be carried out if the must be conducted if the initial assessment of the cri- ticality identifies a corresponding need, but the methodology nevertheless ensures that each process is subjected to at least a high-level analysis and that an appropriate basic assurance is ensured, which automatically leads to a systematically ensured "weakest link" assurance.

Another advantage of a scorecard solution is that it can also be used to query other aspects - for the processes to be controlled operationally - e.g., compliance requirements, checks for documented operating processes, responsibilities for patch and vulnerability management, log evaluation, data backup, authorization concept and others. This can include aspects outside of information security that are necessary from other management systems, e.g., from data protection, compliance or quality management.

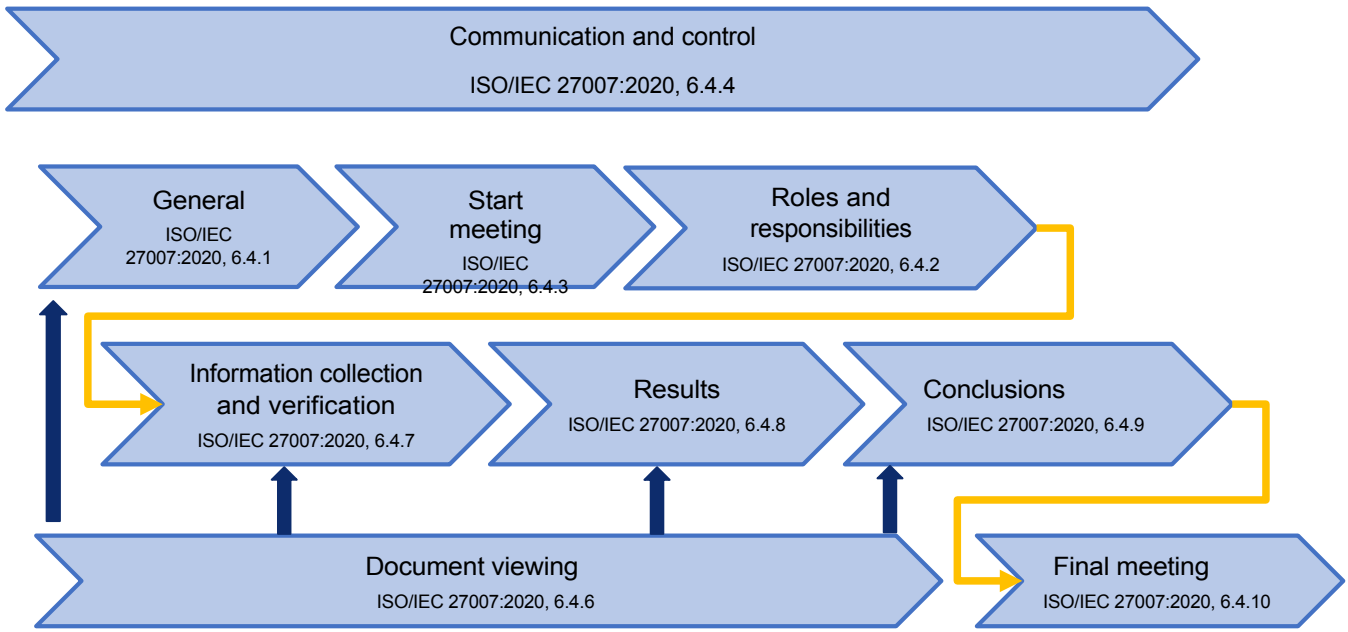
3 See section 3.6

8.4 Internal ISMS audits - mapping to ISO/IEC 19011 and ISO/IEC 27007

Requirements for internal ISMS audits from ISO/IEC 27001:2022 vs. ISO/IEC 19011:2018 & ISO/IEC 27007:2020

Subprocess/activity	ISO/IEC 27001:2022	ISO/IEC 19011:2018 ISO/IEC 27007:2020
Planning of the audit program	9.2 a 9.2 b 9.2 c	5.1 General 5.2 Establishing the audit program objectives
Determination of the audit program	9.2 c	A.5.4 Establishing the audit program
Implementation of the audit program	9.2 c	A.5.5 Implementing the audit program
Monitoring of the audit program	9.2 c	A.5.6 Monitoring the audit program
Review and improvement of the audit program	9.2 c	A.5.7 Reviewing and Improving the audit program
Competence and selection of auditors	9.2 e	7 Competence and evaluation of auditors
Documentation and evidence	9.2 g	A.5.5.7 Managing and maintaining audit program records
Define audit criteria and scope per audit	9.2 d	A.5.5.2 Defining the objectives, scope and criteria for an individual audit
Implementation of ISMS audits	9.2 e	6 Conducting an audit
Reporting of audit results	9.2 f	A.5.5.6 Managing audit program results

8.5 Implementation of internal ISMS audits (process diagram)



ISACA Germany Chapter

Your partner for continuing education:
The ISACA Germany Chapter e. V.

The German professional association of IT auditors, IT security managers and IT governance experts promotes your professional development through exam preparation courses for the international professional certifications CISA, CISM, CRISC and CDPSE.

To support you, we offer a thematically broad certificate program based on the COBIT 2019 framework.

You can find our complete range of courses on our website **www.isaca.de/seminare** view. In addition to classroom seminars, we also offer all courses as **online seminars.**
For all courses you will receive a recognized professional development certificate (so-called CPE hours).