



Implementation guide ISO/IEC 27001:2022

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

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

www.isaca.de
info@isaca.de

Team for English translation 2024:

- Andrea Rupprich (CISA, CISM), usd AG
- Patrick Kernbach, ISecM GmbH
- Stefan Maaß, threategic GmbH
- Holger Schrader, ISecM GmbH (CRISC)
- Ying-Yeung John Man (CISA, CISM)

Team of authors 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 Jeliakov (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)

Management Board

- Markus Gaulke (President, Focus Areas: IT Governance and IT Compliance)
- Thomas O. Englerth (Vice President for Certifications | Acting Vice President for Professional Development)
- Prof. Dr. Matthias Goeken (Vice President for Publications)
- Corinna Kulp (Vice President for Communications & Marketing)
- Dirk Meissner (Vice President for Finance & Administration)
- Sarah Richter (Vice President for Working Groups)

The contents of this guide have been compiled by members of ISACA Germany Chapter e. V. and have been carefully researched. Despite the greatest possible care, this publication makes no claim to completeness. It reflects the opinion of the ISACA Germany Chapter. ISACA Germany Chapter e. V. accepts no liability for the content.

The current guide can be obtained free of charge at www.isaca.de. All rights, including the right to reproduce extracts, are reserved by ISACA Germany Chapter e. V.

Status: September 2026 (final after review and revision by ISACA Information Security Specialist Group)

Implementation guide ISO/IEC 27001:2022

**Practical guide for the implementation of an
information security management system (ISMS)
in accordance with ISO/IEC 27001:2022**

Why this guide?

Information security is indispensable. As an integral part of corporate management, it must be geared towards optimally supporting business objectives. In the current climate of so-called “cyber threats” and the challenges of “cyber security” that are emerging in many places, a well-structured information security management system (ISMS), in accordance with internationally recognised 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 fulfilment of regulations and contractual obligations or the safeguarding of production systems depends on the conditions (e.g. industry, business model or risk appetite) and the specific security objectives of the respective organisation. In all cases, it is crucial to be aware of the information security risks existing in the respective context or to uncover them and to select, implement and ultimately consistently monitor the necessary strategies, processes and security measures.

The actual implementation of an ISMS requires experience but is first and foremost based on the decision and commitment of top management to the topic. A clear management mandate and a security strategy that is aligned with the business strategy, together with competent personnel and the resources that are ultimately always required, are the basic prerequisites for being able to optimally support 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 organisations that either already operate an ISMS in accordance with the international ISO/IEC standard 27001, “Information security, cybersecurity and privacy protection - Information security management systems - Requirements”, or want to set one up, regardless of existing or potential certifications. The guide offers pragmatic assistance and approaches to anyone involved in setting up and/or operating an ISMS. The advantages of a customised and, if necessary, standard-compliant ISMS are clearly highlighted. In particular, practical recommendations for establishing or increasing the maturity level of existing ISMS processes and typical examples of the implementation of various requirements are presented.

Acknowledgement

The ISACA Germany Chapter e.V. would like to thank the ISACA Information Security Specialist Group and the authors for producing this 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

Disclaimer

The information provided here has been compiled to the best of our knowledge by information security experts, auditors and information security officers. No claim is made to completeness or accuracy.

Table of contents

Why this guide?	3
Table of contents	4
1 Introduction	5
2 Structure of the guide	7
2.1 Subject areas	7
2.2 Chapter structure	8
2.3 Conventions	8
3 Building blocks of an ISMS according to ISO/IEC 27001:2022	9
3.1 Context of the Organisation	9
3.2 Leadership and Commitment	10
3.3 IS Objectives	11
3.4 IS Policy	12
3.5 Roles, Responsibilities, and Competencies	13
3.6 Risk Management	14
3.7 Performance/Risk/Compliance Monitoring	19
3.8 Documentation	21
3.9 Communication	23
3.10 Awareness	23
3.11 Supplier Relationships	27
3.12 Internal Audit	29
3.13 Incident Management	33
3.14 Continuous Improvement	35
4 Integration and Operationalisation of Management Systems	37
5 Glossary	39
6 References	41
7 List of illustrations	42
8 Appendix	43
8.1 Mapping Annex ISO/IEC 27001:2022 vs. Annex ISO/IEC 27001:2013	43
8.2 Version comparison ISO/IEC 27001/2:2022 vs. ISO/IEC 27001/2:2013	48
8.3 Holistic safeguarding of the value chain	51
8.4 Internal ISMS audits - mapping to ISO/IEC 19011 and ISO/IEC 27007	53
8.5 Carrying out internal ISMS audits (process diagram)	53

1 Introduction

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

This protection is not an end, but rather serves to support business processes, achieve corporate goals and maintain corporate values through the uninterrupted provision and processing of information. In practice, an ISMS utilises the following three perspectives:

- **G - Governance view**
 - IT objectives and information security objectives derived from the overarching corporate objectives (e.g. supported by or derived from COSO or COBIT)
- **R - Risk view**
 - Protection requirements and risk exposure of company assets and IT systems
 - Risk appetite of the company
 - Opportunities and risks
- **C - Compliance view**
 - External requirements through laws, regulations and standards
 - Internal specifications and guidelines
 - Contractual obligations

These perspectives determine which protective measures are appropriate and effective for:

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

Measures

Measures to achieve and maintain trouble-free information processing must *be effective* to achieve the required level of protection. At the same time, they must also be *economically appropriate (efficient)*.

ISO/IEC 27001:2022 and the systematic and holistic requirements and measures set out therein, which - in varying degrees and quality - are part of the operation of every ISMS, support the achievement of the objectives listed above from all three perspectives (see Figure 1 - Integration of the ISMS into corporate management):

- The *governance view* refers to the control aspects of the ISMS, such as close involvement of the top management level (see chapter 3.2 *Leadership and Commitment*), consistency between the business and information security objectives (see chapter 3.3 *IS Objectives*), the definition of strategies and guidelines (see chapter 3.4 *IS Policy*), an effective and target-group-specific communication strategy (see chapter 3.9 *Communication*), appropriate responsibilities and organisational structures (see chapter 3.5 *Roles, Responsibilities and Competencies*), and targeted monitoring of performance (see chapter 3.7 *Performance/Risk/Compliance Monitoring*). Further information on information security governance can be found in ISO/IEC 27014:2020.
- The *risk view*, which among other things serves as the basis for comprehensible decision-making and prioritisation of technical and organisational measures, is one of the core aspects of an ISMS in accordance with ISO/IEC 27001:2022. It is represented by IS risk management (see chapter 3.6 *Risk management*) and contains specifications and methods for identifying, analysing and evaluating risks in the context of information security, i.e. risks that pose a potential threat to the confidentiality, integrity and/or availability of IT systems, 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 the necessary (security) requirements, supported by the measures in Annex A. On the other hand, it refers to the concrete fulfilment of precisely these requirements, which must be ensured through regular monitoring by management and those responsible for information security (see chapter 3.7 *Performance/Risk/Compliance Monitoring*) as well as through internal audits (see chapters 3.12 *Internal Audit* and 3.14 *Continuous 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 perspective.

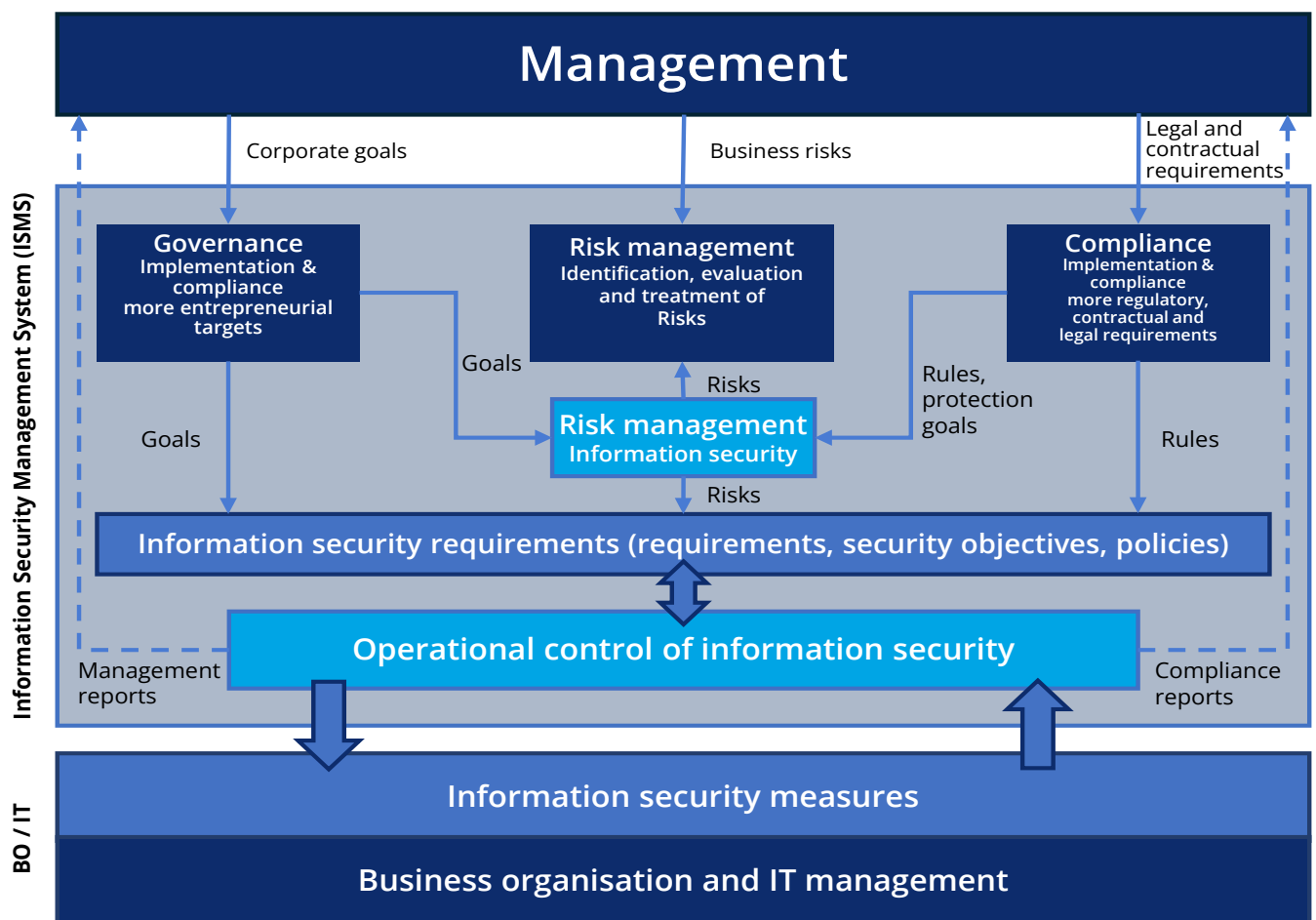


Figure 1: Integration of the ISMS into corporate management¹

¹ Source: Carmao GmbH

2 Structure of the guide

2.1 Subject areas

This implementation guide is based on the key subject areas of the ISO/IEC 27001:2022 standard but does not reproduce the section structure of the standard identically. Instead, the relevant subject areas of an ISMS in accordance with 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 have been restructured and summarised into individual key topics. From the authors’ point of view, the following 14 “building blocks” can essentially be highlighted based on the standard, which together represent the ISMS of an organisation (see Figure 2 - Building blocks of an ISMS according to ISO/IEC 27001:2022):

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

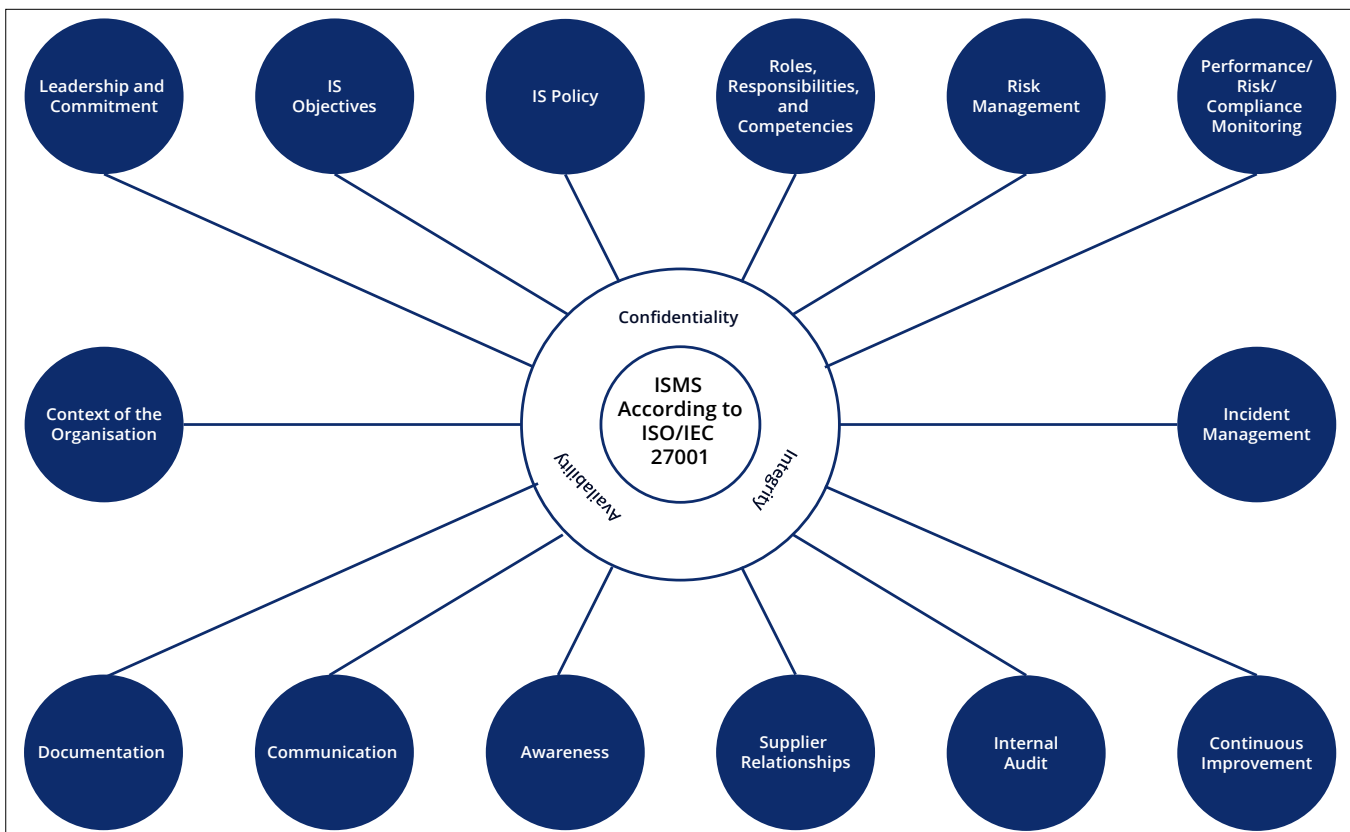


Figure 2: Building blocks of an ISMS according to ISO/IEC 27001:2022

In the following chapters, the key success factors for standard-compliant and tried-and-tested realisation are presented for all components.

As this guide is intended to provide practical assistance, the explanations of the building blocks go beyond the purely standardised content of ISO/IEC 27001:2022 (or ISO/IEC 27002:2022). However, this also means that not every piece of information in this document is equally “suitable” for every ISMS or organisation.

Setting up an ISMS, regardless of whether it is a voluntary commitment or with the intention of certification, is an ambitious project that - like any other project - requires SMART¹ objectives, sufficient and expert resources, a suitable project manager, and a motivated and qualified team. Furthermore, 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 additional norms, standards or other helpful sources, which are labelled as such.

2.2 Chapter structure

The individual chapters 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 and from a practical perspective
- References**
 Indications of the chapter numbers from ISO/IEC 27001:2022 relevant to the subject area as well as further references, if necessary and useful

2.3 Conventions

If the terms “*standard*” or “*norm*” are used in the following without further specification, it always refers to the ISO/IEC 27001:2022 standard.

The term “*chapter*” is used for references within this guideline, the term “*section*” is used for references to the standard.

The term “*Annex*” is used for references to annexes of this guideline, the terms “*Annex*” or “*Annex A*” are used for references to Annex A of the standard.

The terms “*organisation*” and “*company*” each refer to the institution or department within which the ISMS is implemented. The terms are used synonymously in the guidelines. Abbreviations used in the document and further definitions of terms can be found in the Glossary, chapter 5.

¹ SMART: specific, measurable, accepted, realistic, time bounded.

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

3.1 Context of the Organisation

One of the first tasks when implementing an ISMS is to define the specific scope of the management system and to carry out a requirements and environment analysis regarding the organisation and its stakeholders. By considering the context of the organisation, an organisation can ensure that its information security measures are adapted to its specific needs and circumstances and are therefore effective. ISO/IEC 27001 therefore requires organisations to carefully analyse the context of the organisation and integrate it into their information security planning and implementation.

Definition of the scope of application

According to the standard, the ISMS scope must be documented and clearly describe the boundaries of the ISMS within the organisation. It defines which assets (e.g. processes, business areas, locations, and applications) are included in the scope and which are excluded, as well as the interfaces between the ISMS and organisational areas outside the scope.

The scope of application is usually identified with the help of an analysis of the environment and requirements.

- The ISMS scope document defines the boundaries of the information security management system and is an important reference for stakeholders. Upon request, it should be made available so that stakeholders (e.g. customers) can verify whether the processes, infrastructures, topics or requirements relevant to them are covered by the ISMS.
- In practice, organisations often refer to existing ISO/IEC 27001 certificates when responding to enquiries. However, the certificate alone may not provide sufficient information, as the relevant process or service may not be fully covered by the certification scope. To avoid misunderstandings, it is therefore advisable to request not only the certificate but also a clear description of the ISMS scope and, where applicable, the certification scope.
- Another key document is the Statement of Applicability (SoA) required by the standard. The SoA documents the organisation's justified decisions regarding the implementation of the controls listed in Annex A, including whether each control is applied within the ISMS and the reasons for its inclusion or exclusion. The SoA version assessed during the certification audit is typically referenced on the certificate and therefore forms part of the certification documentation.

- It is common for the scope to be at least roughly outlined in the information security policy (information security guideline). In contrast to the scope document, the security policy and the contents of the SoA are usually 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 categorise the ISMS in the overall environment of the scope in question. In addition to the organisational and technical interfaces relevant to the ISMS, it should also describe industry-specific or location-specific conditions. The internal environment, e.g. other management systems (ISO 9001:2015, ISO 22301:2019, etc.), interfaces to other important departments such as risk management, HR, data protection, facility management, auditing and legal; as well as the external environment, e.g. important suppliers and service providers, strategic partners and, if applicable, other organisations, must be considered.

Requirements analysis

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

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

Success factors from practice

As 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, organisational structure, definition of work packages and their prioritisation, project planning) and is also an essential prerequisite for estimating the feasibility and effort (resources, budget, time) for the development and subsequent operation of the ISMS.

- ISO 31000:2018, Section 5.4.1 “*Understanding the organisation and its context*” provides lists that can be used to achieve completeness of presentation.
- The level of detail required to define the scope of application usually results from the internal and external information security requirements of the organisation.
In practice, it has proven helpful to describe the areas significantly affected by the ISMS in sufficient detail in the scope of application, as this description is an important management tool and will be relevant for strategy decisions and (later) co-ordination.
- The identification of stakeholders (and their requirements) required by section 4.2 of the standard must always be carried out carefully and comprehensively, as this is the only way to define clear objectives and content of the ISMS and achieve the best possible benefit. 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 and specifications from supervisory authorities and legislators regarding the affected business processes can serve as the basis for determining relevant internal and external requirements. In practice, this is often carried out by a compliance or IT compliance function, which can provide support in determining the requirements.

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

- Scope of the ISMS (Section 4.3)
- Statement of Applicability (Section 6.1.3 d)
- Overview of all relevant legal, regulatory and contractual requirements that have an impact on the information security strategy and the ISMS (Section A.5.31)
- Overview of all stakeholders relevant to the specific scope of the ISMS

In addition, the following document has proven to be useful in practice:

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

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 introduced by using a top-down approach and establishes a link between business objectives and information security, by considering the requirements of the stakeholders on the one hand and reducing the risks affecting the operational business processes to an appropriate level with effective measures on the other.

In order to fulfil this task, the business objectives and requirements must be known on one hand and, on the other, appropriate organisational framework conditions, such as the introduction or adaptation of risk management processes in the organisation, must be created.

Leadership (in terms of setting a direction and vision), approval and support (leadership and commitment) from the management level are essential when it comes to the necessary adoption of organisation-wide processes, as otherwise the processes introduced in the management system will not be binding and may therefore not be accepted. Managers are therefore responsible here, which is also described as “tone from the top” in view of their role model function.

The standard correctly and explicitly demands that top management must demonstrably assume overall responsibility for information security within the organisation. 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 information security policy (see *Information Security Policy* in Chapter 3.4 *IS Policy*) and a user guideline.

- In the context of IT governance and in connection with management’s responsibility for strategy, the demonstrable assumption of overall responsibility, particularly in regulated areas, is increasingly being demanded by the relevant supervisory authorities¹.

Success factors from practice

Definition of “top management”

“Top management” refers to the management level that is responsible for controlling the organisation to be protected by the ISMS and decides on the use of resources.

- In large companies, “top management”² is not necessarily the highest management level of the entire corporate group (e.g. Group Management Board) from the perspective of the standard. It can also be local management or divisional management that is responsible for the ISMS. The decisive factor is always the specific scope of the respective ISMS.

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 organisation and ISO/IEC 27000:2018, Clause 3.75

- In the case of external certification audits, the certification body may nevertheless require the involvement of the top management level of the entire group of companies (e.g. for reasons of risk liability). For this reason, it is advisable to clarify this point with the certification body in advance if certification is being sought.

Tasks/responsibilities of top management

ISO/IEC 27001:2022 requires top management to set a clear example regarding information security. In practice, this includes a visible engagement and a clear commitment to information security as well as the:

- Exemplary compliance with information security requirements,
- Adequate and clear provision of resources,
- Demanding a role model function from the other management levels,
- Consistent handling of and response to non-conformities,
- 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 specific IS objectives (see Chapter 3.3 *IS Objectives*)
- Definition of decision criteria and principles for risk assessment and treatment and introduction of corresponding 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*)
- Conduct regular ISMS (top) management reviews (see chapter 3.14 *Continuous Improvement*)
- Provision of the necessary human and financial resources to set up the ISMS and implement the information security strategy
- Visibility in awareness events or measures (e.g. leadership video message)

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

- Section 9.3 “*Management Review*” requires documentation of the review of the ISMS by top management, including decisions regarding changes and improvements to the ISMS. These decisions can be recorded as measures in the risk treatment plan.
- During the management review, results, such as decisions made regarding opportunities for continuous improvement, must be retained as documented information.

In addition, the following documents have also proven as useful in practice:

- Derivation and assessment of current risks from identified deviations between strategic IS targets and the degree of target achievement, ideally as a risk treatment plan.
- Evidence of reporting to top management, e.g. in the form of presentations, minutes or reports.
- Reporting on the implementation status, including monitoring the effectiveness of defined measures (especially if they are overdue) from audits, risk treatment, incidents or continuous improvement.

Note: There are various options for documentation in the context of Management responsibility. The examples listed above are suggestions for possible records that help to ensure the traceability of reporting and decision-making. Each organisation must find the form and frequency of documentation that suits it best.

References

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

3.3 IS Objectives

The ISMS as a whole contributes to the protection and maintenance of the required confidentiality, integrity and availability of business processes and the information processed therein. The business objectives defined by the top management serve as the basis for the design and definition of the IT objectives and, more specifically, the information security objectives (IS objectives) and the resulting measures.

Success factors from practice

As the objectives and principles of the ISMS should be derived from the overarching business objectives of the organisation, failure to meet IS objectives can have a direct impact on the achievement of business objectives. It is therefore essential to define appropriate and measurable IS objectives and their implementation.

- The IS objectives must be in line with the contents of the essential protection objectives (confidentiality, integrity, availability; “CIA”) and the IS Guideline (see Chapter 3.4 *IS Policy*).
- The IS objectives should always be aligned with the overarching corporate objectives and regularly reviewed to ensure they are up to date and appropriate. This allows information security requirements to be integrated into operational business activities without being perceived as an additional (or even disruptive) expense. As a result, information security becomes an integral part of work processes.
- When planning the IS objectives, it should be determined how these objectives are to be achieved. This also includes defining the prerequisites for realisation. In addition to the essential activities for achieving the objectives, the necessary resources

and responsibilities, as well as a time frame and a procedure for evaluating the realisation should be defined. In practice, this is often done by making direct reference to planned and ongoing projects. It is crucial that non-functional requirements - and security requirements are non-functional in the majority of cases - are taken into account from the outset and integrated into the planning of projects, products and systems as well as into the further training of employees ("awareness training").

- When formulating IS objectives, care must be taken to ensure that only genuine and long-term objectives/targets are described and not operational technical/organisational measures necessary to achieve the objectives.
- As with any target formulation, it is advisable to formulate SMART³ targets when setting IS targets and to coordinate these with the relevant levels of responsibility.
- The degree of achievement of the information security objectives should be measurable. Ideally, this can be measured using KPIs defined in advance. Practical support for this task is provided, for example, by the ISACA practical guide "Evaluation of the performance of an ISMS through key indicators" or COBIT 2019 Focus Area: Information Security.
- In practice, formulating meaningful, measurable objectives and implementing the measurements required to achieve them can be a challenging endeavour. It is therefore advisable - especially at the beginning of an ISMS implementation - to initially define a small number of IS objectives that make sense for the respective organisation and are balanced in terms of implementation costs and benefits.
- The measurability of IS objectives is "only" required by the standard if there is a corresponding practical feasibility. In practice, "if practicable" is generally understood to be less stringent 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).

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

- Documentation of IS targets must be kept available.

In addition, the following points have proven to be effective in practice:

- The 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 the IS objectives are to be achieved through specific projects.
- The degree of realisation of the IS targets is shown by key figures, 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., Practical guide "Evaluation of the performance of an ISMS through key indicators" (https://www.isaca.de/images/Publikationen/Leitfaden/ISACA_KPI_Guide_2024.pdf)

3.4 IS Policy

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

The policy must be suitable for the purpose of the organisation and include the intended principles and objectives of the ISMS, as well as the organisation's general information security objectives.

Success factors from practice

The policy is an important tool for the organisation, through which the responsible management can communicate the importance of an effective ISMS and compliance with the ISMS requirements. The policy also sets out the key strategic and tactical objectives that are to be achieved with the help of the ISMS. Ideally, the effects and requirements that arise for the relevant personnel and the respective business areas within the scope of application are also presented.

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

- The IS policy must be approved by the highest management level (top management) and made available to the responsible supervisory bodies.
- The IS policy must be available as documented information and be subject to comprehensible document control.
- The IS policy can include a reference to the corporate objectives and other relevant specialised objectives such as the IT objectives.
- The language of the IS policy must correspond to the company's practices and emphasise the importance of the document in the best possible way.
- As part of employee awareness, it must be ensured that all affected employees within the scope of application are aware of the IS policy and related requirements and specifications. It must be communicated to the employees concerned and be made available to stakeholders, if required (see Chapter 3.10 *Awareness*).

³ SMART: specific, measurable, accepted, realistic, time-bound.

- To achieve the objectives in practice, it is important that the individual employees are aware of their personal responsibility and involvement in processes in the context of information security and know the associated specific requirements (which are derived from the IS policy and are reflected, for example, in topic-specific guidelines and work instructions).
- The IS policy should not be mixed with more extensive documentation and implementation specifications, such as the contents of security concepts or manuals. However, reference may be made to the guideline (or other relevant high-level documents of the ISMS) in such “downstream” documents to achieve consistency in the “chain of requirements”.
- Depending on the chosen approach of the ISMS and the existing structure and work organisation within an organisation, it may make sense to design the IS policy as a top-level document, i.e. comprehensive overall document on the topic of information security or, if necessary, to place it 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 appropriate wording and scope for the objectives of the IS strategy.
- If the ISMS documentation is divided into a main document and other detailed documents, a division of responsibility in favour of flexible change management can be useful. For example, top management is responsible for the IS policy, while the information security officer or relevant departments can be responsible for the detailed documents.
- Although many templates and text modules can be used when searching online, it is advisable to create the IS policy as a new/dedicated document that best meets the individual requirements of the organisation. Templates can provide ideas and suggestions for structuring and possible content. However, it is crucial for the success of implementation and the identification of employees with the topic of information security that the guideline is visibly oriented towards the company and subordinate specialist objectives and that the core statements allow the reader to recognise a connection to the organisation concerned.

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirement apply:

- Information security policy (see Section 5.2 e)

In addition, the following documents have established themselves as useful in practice:

- Topic-specific information security guidelines (see Annex A 5.1)
- Accompanying documents and organisational charts, for example to clarify the organisational structure in the context of information security (if not included in the guideline)

References

ISO/IEC 27001:2022 - Section 5.2, A.5.1

3.5 Roles, Responsibilities, and Competencies

According to Section 5.3 of the ISO/IEC 27001:2022 standard, the organisation 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 also be identified and be made available (see Section 7.1, ISO/IEC 27001:2022).

In this context, management must also assign and communicate the responsibilities and authorisations for tasks that are relevant to information security. Care should be taken to ensure that the responsibilities of the roles are clearly regulated and defined and that any conflicts of interest are avoided (e.g. with the help of a RACI⁴ or SoD⁵ matrix).

Success factors from practice

Specification of roles within the ISMS organisation

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 authorisations that are 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 ISMS⁶.

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

- The role description of the ISO/CISO must also include the necessary competencies (experience, education, training, social skills, etc.) required to perform the role. For this purpose, it is advisable to use a job description or a letter of appointment listing the assigned tasks.
- Conflicts of interest that should be avoided in practice at all costs:
 - (Chief) Information Security Officer and IT Manager/CIO⁷
 - Data Protection Officer (DPO) and IT Manager/CIO
 - Internal ISMS auditor and IT administrator
- In practice, the two roles of ISO/CISO and DPO can also be performed by a single employee under certain conditions. However, this combination is also associated with certain (unavoidable) potential conflicts. For example, the DPO is pro-

4 RACI: Responsible (responsibility for implementation), Accountable (overall responsibility), Consulted (technical 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 CIO: Chief Information Officer.

tected by law regarding their actions and is subject to a duty of confidentiality. However, they cannot automatically transfer this protection or duty to the role of CISO. There is also a legal discussion regarding the guarantor duty of the CISO or compliance officer, etc. This does not apply to the DPO. A personal union of these tasks can therefore lead to a substantial conflict of interest in the worst case and should therefore be analysed and weighed up in detail.

- Depending on the size and business activities of the organisation and the specific scope of the ISMS selected, the combination of the DPO and CISO roles can also result in synergies that would not exist if the roles were separated (e.g. in terms of information flow, overview and design of measures). However, it must always be carefully checked whether the candidate in question has the necessary professional and personal skills and can actually fulfil the workload in both areas. On the other hand, as already mentioned, it must be carefully considered whether the conflicts of interest that may arise are “manageable” and would not lead to any serious disadvantages in the fulfilment of (one of) the two functions.
- Another example of possible conflicts of interest between the DPO and CISO concerns the collection and analysis of traffic and log data. While the DPO will typically only authorise the collection and analysis of personal data or data that can be linked to personal data under very specific conditions and for specific purposes, the CISO would like to make the best possible use of technical measures to increase the level of security (preventive protection) and to identify and analyse potentially damaging events (detective protection).

The organisation must ensure that all persons have the required competencies through appropriate education, training or experience. The organisation must be able to provide evidence of the existence of competencies, e.g. via corresponding training certificates in the personnel file (training history) of the respective employee (see Section 7.2 d).

- ISO/IEC 27001:2022 provides a rough framework for the security organisation of companies (e.g. top management, risk owner, auditor) but does not describe in detail how roles and responsibilities should be assigned in practice.
- It has proven to be advantageous to select employees for the required roles within the ISMS who already have an “innate” affinity for the topic of information security or have sufficient intrinsic motivation. In addition to specialist knowledge, the CISO/ISO in particular, requires social skills, goal-oriented communication behaviour, integrity, the ability to persuade, and successful conflict management. Many of the tasks that arise in connection with the implementation of the information security strategy and (sometimes unpleasant or unpopular) associated measures cannot otherwise be solved satisfactorily.
- One of the most important characteristics of a CISO is also the ability to “translate” between corporate objectives and compliance requirements on the one hand and information security risks and measures on the other.

- The role of the CISO requires leadership skills and should have the same status as that of a manager in the company.
- Examples of organisational structures regarding information security can be found in “COBIT 2019 Focus Area: Information Security” and “BSI Standard 200-2 - IT-Grundschutz-Methodology”. These describe, among other things, the roles and responsibilities of the CISO, the steering committee, the information security manager, the roles in the risk management process and the functional data owners.

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

- Proof of competency (Section 7.2 d)

Furthermore, the following documents have been found to be useful in practice:

- Role descriptions, including the necessary reporting to top management (see Section 5.3b)
- Job profiles/letter of appointment
- Organisation of strategic and operational cooperation between 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 Management⁸

An IS risk describes the possibility that a specific threat exploits vulnerabilities in an information system, an application system or (parts of) the IT infrastructure, which represents a breach of information security (confidentiality, integrity or availability) and thus leads to negative effects on, among other things, the business activities, financial targets, or reputation of an organisation.

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 management 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* or *sustainable* improvement in the existing *level of security within the scope* of the ISMS.

⁸ This chapter relates exclusively to risk management in the context of information security.

The aim is to reduce the identified risks and avert intolerable damage to the organisation in question or reduce it to a level that is acceptable for the company. What is considered *acceptable* must be decided by those responsible 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: Unacceptable damage to the organisation in question must be prevented or reduced to a level that is deemed acceptable by the company.

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

- Recognising and eliminating information security risks at an early stage
- Establishment of standardised assessment methods for identified risks
- Clear assignment of responsibilities when dealing with risks
- Standardised and clear documentation of risks, including their assessment
- Efficient treatment of risks⁹

Basics of IT risk management and procedure

How do risks arise?

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

- Data exchange within and outside the organisation
- Adaptation of internal organisation and cooperation (especially for larger companies)
- (Existing) systems and applications that cannot be updated or replaced
- Cooperation with external partners/service providers
- Remote access to the company 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 systems and technologies (e.g. cloud and mobile devices)
- Entry into new markets (geographical and product-related)

While it is imperative to consider all sources and influencing factors, each organisation must define individual risk management priorities based on its respective business activities and the related internal and external requirements.

- Efficient risk management can only take place if the risk exposure and the environment of the respective business activity are analysed first. In order to identify potential risks, it is essential to first understand the existing risk areas and conduct a thorough assessment of these. A useful starting point for this would be, for example, a process map or an environment analysis (see Chapter 3.1 *Context of the organisation*).
- ISO/IEC 27005, for example, can be used to support the formulation and organisation of the risk assessment process. In addition to the well-developed main section, the appendices also contain valuable information on implementation.

Detection and assessment of risks

Before the actual identification and treatment of risks can begin, both the generically formulated risk assessment process and the company-wide or ISMS-wide risk acceptance criteria must be defined in consultation with the highest management level (top management – unless these can or must be adopted from a higher-level risk management system).¹⁰

The risk assessment process includes the following:

- Methods for risk identification
- Criteria for assessing risks
- Risk acceptance criteria

Apply methods for risk identification

The identification of relevant risks usually requires the views of several stakeholders or departments to be taken into account and brought together. Various techniques and methods can be used as tools, such as¹¹:

- Interviews
- Scenario analysis/what-if analysis
- Brainstorming
- Business impact analysis (BIA)
- Checklists
- Delphi method
- STRIDE Threat Model (Microsoft)

Example

When analysing the risks of a new e-commerce web application, the people involved bring up different risk aspects for discussion. The software developer sees weaknesses in the chosen

⁹ For example, by adapting the security strategy or implementing appropriate security measures.

¹⁰ In ISO 31000:2018, these activities are described in section 6 “Process”.

¹¹ See also IEC 31010:2019.

programming language that can be mitigated by (automatic) code reviews, for example. The IT administrator expresses their 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 organisational measures to fulfil the requirements of Art. 32 (1) GDPR. The information security officer, in turn, recognises the scope of the project (impact in the event of availability restrictions or data outflow) and therefore requests a penetration test before going live.

- This example has not been taken from a textbook. However, it demonstrates that conducting a risk analysis can also go hand in hand with the direct formulation of (counter) measures.
- If the risk management process is highly dynamic, the direct formulation of (counter) measures can be used to initiate risk management promptly. If, on the other hand, the risk management process is implemented with low momentum, this can also be deliberately avoided to first complete the analysis in full/comprehensively and then defining further activities at a later stage.
- With a “compact” or “dynamic” risk management process, which quickly leads to the discussion and selection of treatment options, there is a danger that the process will tend to be reactive and action-centred and that the analysis of risks may be neglected as a result.
- The most suitable approach should be chosen depending on the size and scope of an organisation or specific project!

Define criteria for assessing risks

The criteria for assessing risks must be formulated in such a way that they can be used for the widest possible variation of risk types or risk categories. Whether a points model or a catalogue 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 to provide a set of questions tailored to the organisation’s business activities in addition to the classic criteria (such as protection requirements for confidentiality/integrity/availability, supported business processes, number of users), which can be supplemented individually for each use case.
- Assessing the probability of occurrence (see “Step 2: Risk analysis” below) is quite challenging in practice. In addition to “looking back” (empirical values, comparable events in other organisations, key figures, statistics, etc.), it is also essential to “look ahead” to take into account previously “unknown” findings and developments that may already be on the horizon (e.g. the emergence of new technologies or changed hazard situations)¹². Or, to put it another way: “In risk management, success depends on previous preparation.”¹³

Define risk acceptance criteria

Defining risk acceptance criteria is a central task in the risk management process, as this is the only way to ensure that the organisation does not have to treat all identified and assessed risks “equally” in a cost- and resource-intensive manner.

- Risk acceptance criteria can be defined in the form of acceptance levels depending on the qualitative and/or quantitative damage potential (e.g. non-compliance, financial damage, reputational damage, impairment of task fulfilment).
- Risk acceptance criteria may include several thresholds. Each threshold level can be linked to a specific hierarchy/management level, so that risks above a certain level are only accepted by the designated managers within that level.
- For better comparability, qualitative damage levels can be converted into quantitative (financial) amounts. However, this is generally only possible as an approximation.
- It can be useful - especially for small and medium-sized companies - to start the risk assessment 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 technical experts from the IT department(s) and specialist department(s), even without a fully developed model. The risk acceptance criteria can then be gradually derived from the results and converted into formal criteria at a later stage - after approval by the company management.
- When defining risk acceptance criteria, it is important to proceed with circumspection and foresight in order to adequately reflect the company’s risk appetite¹⁴ (neither too high nor too low) and at the same time ensure the efficiency and effectiveness of the ISMS by identifying risks “across the board” and treating them consistently according to their assessment and, for example, in accordance with legal or regulatory requirements (not every risk can be treated as a top priority).
- In practice, it is a major challenge to implement a truly comprehensive risk management system that identifies and analyses all information security risks in all areas of the company and its processes in detail is a major challenge.

Orientation towards an established risk management process

Once the risk assessment has been defined, the next steps in the risk management process are iterative. Using an established process as a guide serves to ensure transparency and traceability and makes the results of the entire process more reliable. ISO 31000 focuses on the following steps:

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

¹² For example, through APTs or zero-day vulnerabilities.

¹³ Based on Confucius, Chinese philosopher, *551 BC †479 BC.

¹⁴ The greater the risk appetite, the more room for manoeuvre and opportunities are generally available.

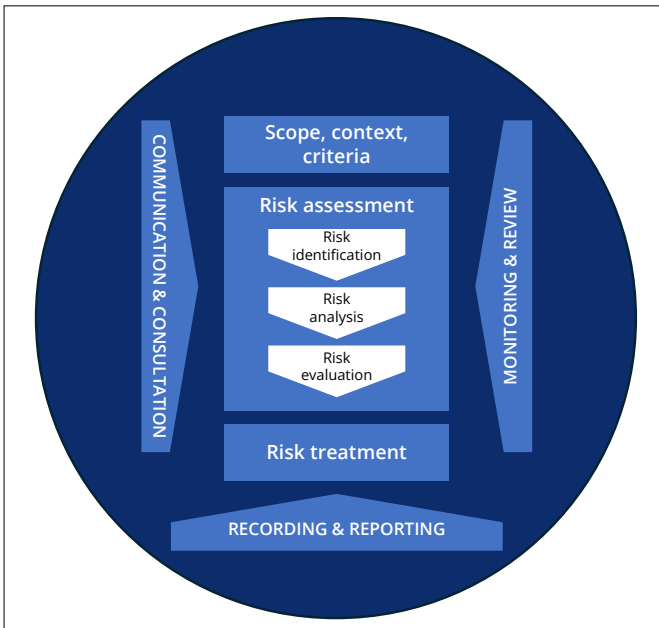


Figure 3: Risk management process according to ISO 31000¹⁵

Step 1: Risk identification

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

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

- Risk analysis
 - Explicit risk analysis and assessments are carried out for business-critical processes, applications and systems. Based on these, clear statements can be made regarding the risk situation and risk exposure of the processes or applications/systems concerned.
 - Risk analysis (with an adapted scope in each case) should be included as a mandatory element within project management.
- Audits
 - Audits carried out show that security standards and known best practices are not or not sufficiently fulfilled by the responsible bodies or in systems.
 - The prerequisite for this is, of course, that audits are actually carried out (see 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 business
 - New, previously unknown risks may come to light as a result of findings during “normal” operations, which should/must be reported (promptly) to risk management by the specialist team or employee, depending on the risk management process selected.

■ Security incidents

- Security incidents (whatever the definition of “security incident” may be) can identify previously unknown risks that become visible because of the incident. On the other hand, risks that were already known but not sufficiently addressed or previously accepted can actually materialise (for example, through active exploitation of an already known vulnerability by an attacker or the failure of a system due to inadequate technical dimensioning).

Step 2: Risk analysis

When analysing identified risks, both the likelihood and the possible consequences if the risks materialise should be clearly worked out and presented to the decision-makers in a comprehensible manner.

- When formulating the consequences in natural language, care should be taken to emphasise the consequences for business processes and business activities rather than technical details.
- Standardised evaluation matrices can be used for risk analysis, although it may make sense to use matrices with an even number of columns (e.g. 4x4) depending on the organisation and application. When using matrices with an uneven number of columns/rows (e.g. 3x3 or 5x5), there is a fundamental risk that the decision will often be made in favour of “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, as they can assess the impact of the occurrence of the risk and are ultimately responsible 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).

- It is at this point that the importance of identifying and defining the risk owner as part of the overall risk management process becomes apparent.
- In practice, the role of the risk owner should be filled by the appropriately designated responsible persons or managers of the company (e.g. board of directors, managing director, managing director, division manager, head of department or group leader). In the case of projects, the project manager usually fulfils the role of risk owner, at least for project-specific risks.

Step 4: Risk treatment

Risks are treated according to the risk appetite of the respective organisation. In the context of information security, the ISO/IEC 27005 models are particularly suitable as a starting point for modelling risk treatment options¹⁶.

¹⁵ See ISO 31000:2018

¹⁶ See, for example, section 8 of ISO/IEC 27005:2022 - “Information security risk treatment”.

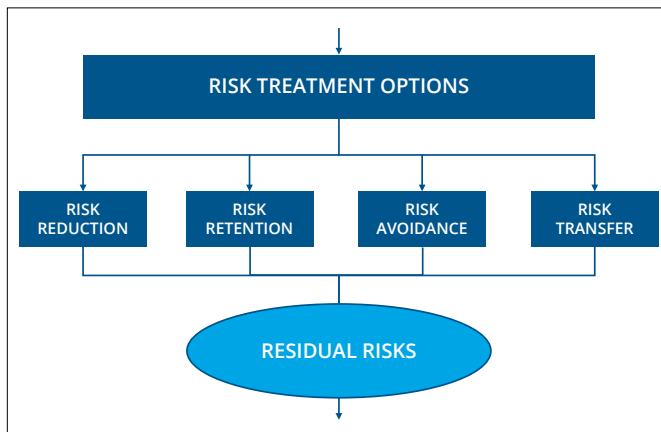


Figure 4: Risk treatment options according to ISO/IEC 27005

- Risk treatment measures can in principle be taken from all sources but must be harmonised with Annex A of the Standard and the SoA of the ISMS.
- Risks must be assigned to the corresponding risk owners. Without dedicated, responsible owners, both the “correct” assessment and the sustainably successful treatment of identified risks are made more difficult.
- The risk owner is usually the entity that must bear the economic impact when the risk materialises. In many cases, this is the process owner, but depending on the impact and risk assessment, it can also lie with higher management.
- Even if risks are caused by IT systems, for example, the business units concerned ultimately bear the consequences. This means that although (IT) risks must be handled by the respective¹⁷ IT department (responsibility), the risk ownership and overall responsibility still lie with the relevant departments, which must also decide on the provision of resources (accountability).
- The identification of risks and the identification of the associated risk owners can take place separately or at different times.

Documentation and reporting

- It is advisable to keep the results of all risk assessments in a central location, e.g. in the form of a risk register. Although this is not a standard requirement, it helps to analyse and manage known risks and their processing status.
- Depending on the size of the organisation, tools with different functionalities are required (number of risks, number of users, authorisation concept, multi-client capability, online availability, evaluation options, etc.).
- The standard does not require a centralised risk register. However, it does require that the risk assessment process for information security risks leads to consistent, valid and comparable

results (see Section 6.1.2 b). Therefore, depending on the type and utilisation of the tools used, creating a register is a logical consequence.

- As the risk register usually contains sensitive and (strictly) confidential information, a customised rights and roles concept for data access should be created and implemented.

Success factors from practice

- If the company or group of companies already has an overarching risk management system, IS risk management should be integrated into this system (e.g. as part of operational risk management) or at least have defined interfaces.
- Where possible, risk management should be process-oriented instead of focusing on the individual assets. On the one hand, this ensures that risks and hazards are formulated in a (business) process-orientated 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 or expanded so that a risk analysis and assessment (of varying intensity depending on the type and scope of the project) must be carried out. The project team must document the results of the analysis and - depending on how risk management is structured - 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.
- It is also advisable to introduce risk analysis and assessments as a mandatory part of change management for (extensive) changes to processes, applications or systems.
- If non-conformities or vulnerabilities are identified (e.g. through monitoring or other operational IT processes such as change, problem or incident management) that cannot be rectified within regular operations or cannot be rectified in a timely manner, these must be assessed in risk management and dealt with by the risk owner.
- Risk analysis and assessments always require the specialist expertise of the respective process owner. The organisation’s IS officers can assist with the implementation and, for example, record the risks in interviews or workshops and make suggestions for the assessment. 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 pair of eyes”. It is crucial that there is a formal and pragmatic process that optimally supports the specialist departments and project managers in their work and at the same time ensures that risks are recognised at an early stage and dealt with appropriately.
- BSI Standard 200-3 – Risk analysis based on IT-Grundschrift – provides starting points for how a risk analysis for information processing can be carried out using the threats listed in the IT-Grundschrift compendium. However, the BSI methodology requires that the steps of the IT-Grundschrift methodology

¹⁷ This also includes specialist departments and software development departments, which may be located outside IT, are responsible for their own IT risks and are responsible for their risk management.

have first been carried out (including information network, structural analysis, protection requirements assessment, modelling, 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 this is not necessary.

- In the context of an ISMS, the asset worth protecting always remains the information itself. It is the task of the respective responsible parties (company management, management, process owners) to evaluate this asset regarding 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. The ISMS managers are the “guardians” for the implementation of the information security strategy and are responsible, among other things, for truthful reporting regarding risk exposure and security incidents.

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

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

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

- Further records and results of risk assessments and risk analysis

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 Performance/Risk/Compliance Monitoring

In the context of the ISMS, several requirements are defined, e.g. information security objectives or guidelines and concepts for their implementation in practice. It is expected that these requirements will be met, which will be ensured by means of appropriate monitoring. “Performance/risk/compliance monitoring” therefore also includes the continuous monitoring and improvement of the information security management system (ISMS).

- Performance monitoring comprises the evaluation of the effectiveness of the ISMS regarding the achievement of the security objectives and the fulfilment of 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 refers to the monitoring of compliance with legal requirements and regulatory provisions, as well as internal guidelines and standards.

By carrying out performance, risk and compliance monitoring, organisations should ensure that their ISMS works effectively and efficiently and that the requirements of ISO/IEC 27001 as well as legal and regulatory requirements are met. It involves regularly reviewing ISMS processes, procedures and controls to ensure that they meet the relevant requirements.

To ensure comparability, continuity and traceability, all targets whose achievement is to be measured using key figures should fulfil the SMART criteria:

- Specific
- Measurable
- Achievable / Accepted
- Realistic / Relevant
- Time-bound

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

The information security officer is now able to evaluate and manage information security using the various KPIs, e.g. with the help of a dashboard view. From the large number of KPIs, we focus on the following KPI classes regarding information security:

Key indicators KxIs (key performance/risk/control indicators)

KPI - Key Performance Indicators

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

KRI - Key Risk Indicators

A key risk indicator is a metric (target/actual comparison) that shows whether changes in the risk profile potentially exceed the desired tolerance limits and therefore jeopardise the achievement of objectives. It is therefore a measure of how **risk-orientated**

a company implements the relevant measures and information security processes. A situation that exceeds the company's risk appetite is brought back into the acceptable risk range through countermeasures.

KCI - Key Control Indicators

A key control indicator is a metric (target/actual comparison) that shows how **effectively** a company implements the relevant measures and information security processes in terms of target achievement. A measure is effective if the control objectives are reliably achieved within the desired tolerance limits.

These key indicators should be used in practice to continuously monitor the effectiveness and efficiency of the ISMS processes and the established measures. They provide information on the performance status of the entire ISMS and serve as a trigger for necessary management intervention.

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

The benefit of KxIs lies in the ability to provide basic information about the management system. They provide management with a comprehensible and understandable basis for making well-founded decisions on managing information security. In addition to traditional performance analysis, KxIs can be used to uncover indications of (new) risks or changes within the risk landscape as well as non-conformities regarding the implementation of security requirements and guidelines.

Success factors from practice

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

- Each key indicator must be measurable, repeatable and comparable, in terms of time, organisation and industry.
- Indicators should be systematically structured and based on solid and appropriate statistical and mathematical foundations with reliable measurements of sufficient scope.
- The indicators should be timely and reflect current information. The frequency of data collection and the duration of processing until presentation to management should enable control, similar to the displays on the dashboard of a car, which tell the driver of the system whether all important parameters are within the desired, proper range.
- Performance indicators must be relevant to the objectives of information security management, enable steering interventions and provide practical support for decision-making.
- The selection of indicators should be risk-based, and the cost-effectiveness of data collection should be balanced against its informative value and usefulness for decision-making.
- The selection of KxIs should enable an assessment of the ISMS as a whole. This means that it is not sufficient to only record individual sub-aspects and indicators. Rather, these must be summarised into a meaningful whole and record the performance of the entire ISMS.
- Performance indicators can also be used to evaluate and manage service provider relationships and can, for example, be included as part of a contract or in a (security) SLA.

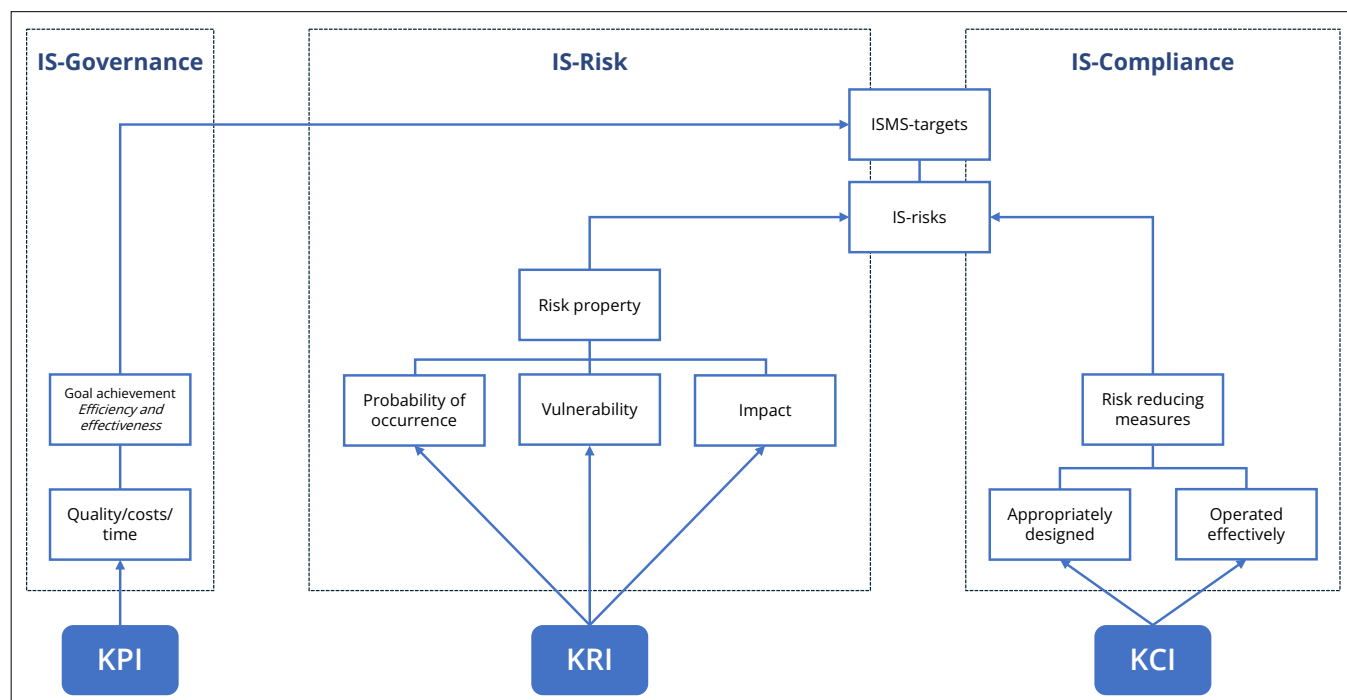


Figure 5: Structure and relationship of KPI, KRI and KCI

- See also Appendix 8.3 (Holistic safeguarding of the value chain page 64)

Relevant KxIs for the ISMS

There are many sources for information security performance indicators that offer a huge selection, such as COBIT 2019 for Information Security¹⁸, The CIS Security Metrics¹⁹ or Performance Measurement Guide for Information Security²⁰, to name just a few.

Of course, we would also like to take this opportunity to refer you to the ISACA practical guide “Evaluation of the performance of an ISMS through key indicators” (for a target oriented IS KPI system in accordance with ISO/IEC 27004:2016”).

The specific selection of KxIs should be based on the circumstances of the respective organisation, fulfil the quality criteria already described and be continuously optimised.

Below are some examples of such key indicators from the ISACA practice guide for assessing the performance of an ISMS through key indicators:

Key performance indicators

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

Key risk indicators

- Percentage of employees who click on a prepared phishing link during an awareness campaign.
- Percentage of IT systems with vulnerabilities that were not closed within the planned time frame.
- Percentage of productive IT systems that are no longer supported by the provider.

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 have passed the assessment/self-assessment at the end of the awareness campaign compared to the number of employees already trained in an awareness campaign.

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

- Documentation of the measurement structure for all KxIs. It answers the following questions:
 - What was measured and evaluated?
 - Which methods were used for measuring, analysing and evaluating and do they lead to reproducible results?
 - When was it measured and by whom?
 - When was it analysed and evaluated and by whom?
- Results of the measurements and the resulting management reports on escalation

Furthermore, the following documents have been found to be useful in practice:

- All records and evidence that contain information relevant to the context of effectiveness monitoring, as the organisation must retain 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

ISACA - Evaluation of the performance of an ISMS through key indicators

3.8 Documentation

In the context of documentation, a central requirement within the management system is to ensure that (at a minimum) the following aspects are regulated for the ISMS documentation:

- Documents must be created, updated, authorised and, if necessary, communicated according to a defined procedure (workflow).
- Documents must be clearly labelled, e.g. title, date, author, version, storage as well as an appropriate suitability and suitability test (QA) and final approval.
- Classification of documents and their contents regarding confidentiality.
- Creation of sufficient and relevant records as part of operational activities to ensure traceability.

The content and level of detail of the documents required by the standard are influenced by the chosen scope of the ISMS, the size of the organisation, the technologies used and the organisa-

¹⁸ ISACA, COBIT 2019 for Information Security, 2019

¹⁹ The Center for Internet Security, “The CIS Security Metrics”

²⁰ “Performance Measurement Guide for Information Security”, NIST Special Publication SP 800-55

tional structure, among other factors, and therefore may differ from organisation to organisation.

The number and type of documents also vary. From a practical perspective, it may make sense for one organisation to create a set of (many) individual documents and maintain them granularly. For another organisation, on the other hand, it may make more sense to use a central storage medium that can be accessed organisation wide. 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 “documented 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 must be checked on an ongoing basis to ensure the following:

- ▶ Availability and suitability for use, regardless of time and place.
- ▶ Adequate protection, e.g. against loss of confidentiality, improper use or unauthorised manipulation/loss of integrity.

Success factors from practice

In practice, the fulfilment of the requirement for document control can generally be supported with a document guideline. However, the key to successful implementation is not the quantity of documentation, but how its quality, acceptance and availability as well as how efficiently it is controlled (keyword: document control).

Practical aspects for assessing documentation quality and document control arise from the following questions:

- ▶ How are the contents of and changes to the documentation communicated or how employees are made aware of changes?
- ▶ How familiar are employees with the content of the documents and how do those affected utilize the requirements on a day-to-day basis?
- ▶ Who knows the storage locations and storage media where the current documents can be found?
- ▶ Is the content prepared with the target group in mind and clearly formulated?
- ▶ How easy is it for new employees to grasp the contents of the documents and implement them in their own working environment? What kind of questions are there?
- ▶ Are the documents updated regularly or on request? How well does the updating and release of documents work?
- ▶ Are there dedicated document owners for each document?

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply (Sections 4-10):

- ▶ Scope of the ISMS - (Section 4.3)
- ▶ Information security policy - (Section 5.2 e)
- ▶ Description of the information security risk assessment process - (Section 6.1.2)
- ▶ Description of the information security risk treatment process - (Section 6.1.3)
- ▶ Statement of Applicability - (Section 6.1.3 d)
- ▶ Information security risk treatment plan - (Section 6.1.3 e)
- ▶ Information security objectives - (Section 6.2)
- ▶ Monitoring the achievement of information security objectives - (Sections 6.2 d, 6.2 g)
- ▶ Evidence of competency - (Section 7.2 d)
- ▶ Evidence of correct execution and changes to ISMS processes²¹ (Operational planning and control, Section 8.1d; Planning of changes, Section 6.3)
- ▶ Results of the information security risk assessment - (Section 8.2)
- ▶ Results of the information security risk treatments - (Section 8.3)
- ▶ Evidence of the monitoring and performance measurement results of the ISMS - (Section 9.1)
- ▶ Evidence of the audit program(s) and the audit results - (Section 9.2)
- ▶ Evidence of the results of management reviews - (Section 9.3)
- ▶ Identified nonconformities with ISMS requirements and actions taken to address 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 - (Section 10.1 g)

Furthermore, the organisation must determine for itself what documentation and records are necessary in addition to those required by the standard 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 visualised using suitable process representations (e.g. event-driven process chains, EPCs) and communicated to employees in a comprehensible manner using process descriptions or, if necessary, specific work instructions.

²¹ In this context, the standard refers to “documented information to the extent necessary”.

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 organisations and departments is required (e.g. suppliers, HR department, legal department, internal audit). 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 organisations (see also environment analysis in Chapter 3.1 *Context of the organisation*). Internal communication refers to the need for communication within the management system and within the organisation, e.g. with internal stakeholders such as the Executive Board, managers and employees.

As part of an analysis, it should be determined which information in the context of the ISMS (Section 7.4 a of the standard) must be communicated by whom (Section 7.4 d) to whom (Section 7.4 c). In addition, it should be determined when communication should take place (Section 7.4 b) and via which communication channels/processes (Section 7.4 e).

Ideally, the results of the analysis are summarised in a communication plan. This is usually formally developed in five specific steps:



Figure 6: Development of a communication plan

- Process and communication interfaces should be clearly defined in terms of efficiency and integrated into the organisational and operational processes. It must be clearly regulated which information must be provided by whom to whom and at what time, for example as part of change or incident management.

- The standard requires the organisation to determine internal and external communication in the context of the ISMS. It does not explicitly require this to be done as part of an analysis. However, the practical benefit of an analysis is that it can be used to clearly identify the requirements for a customised communication structure.

Success factors from practice

A communication plan, also known as a communication matrix, can look like the following, as an example:

- Once the communication matrix has been developed, it has been shown in practice that various interfaces between communication partners and/or departments already informally exist. Identifying these is an important success factor to efficiently organise communication in the context of the ISMS within the organisation. It may make sense to integrate the IS communication plan into an overarching communication plan.
- In order to be able to communicate with all levels of the organisation, a platform should be provided so that the comprehensive security information of the ISMS is accessible to different target groups. Collaboration platforms for better communication and reporting could be, for example, the intranet, Confluence, a wiki or similar.

Documentation requirements

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

The following documents have been found 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 most frequent and major misconceptions that jeopardise the security of a company’s information and IT systems, as a large number of security-relevant events and security incidents in operations fall into the categories “lack of a sense of responsibility”, “lack of or immature processes” and “inadequate training and/or sensitivity of employees”.

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

Internal communication				
Communication reason	Initiator	Receiver	Frequency	Medium
Management review	CISO	Top management	Yearly	Management report according to template by e-mail + presentation
Reporting	CISO	Top management	Quarterly	KPI report according to template by e-mail + presentation
Awareness training	CISO	All employees in the area of application	Yearly	Training (presence/online)
IS-Newsletter	CISO	All employees within the scope of application	Quarterly 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 the event of an acute threat, project-related	Balanced scorecard report, if necessary, by e-mail
Security incident	Support	CISO (possibly others according to SIRP)	Case-related	Escalation in accordance with SIRP (Security Incident Response Process)
Security incident	CISO	Top management	Case-related	E-mail, verbally if necessary
Security incident involving 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
ISMS Jourfix	ISMS Team	ISMS Team, relevant Stakeholders as needed	monthly	meeting record

Table 1: Communication plan – Internal communication

External communication				
Communication reason	Initiator	Receiver	Frequency	Medium
Report operating service provider	Operational service provider	CISO	Quarterly	SLA report according to template by e-mail
Externally commissioned CERT/ Vulnerability Analysis	CERT	CISO/IT Manager	Weekly/ case-related	Report according to contract by e-mail
Security incident	CISO, possibly top management	Customers/partners affected	Case-related	According to SIRP, on website, letter, e-mail, telephone
Security incident with a criminal background	CISO	Investigating authorities	Case-related	According to SIRP

Table 2: Communication plan – External communication

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 guidelines and user guidelines as well as the relevant information security guidelines must be ensured on the part of the recipients of the guidelines (employees, managers, external partners).
- The contribution of each employee within the ISMS scope should be based on the measures documented in the user guideline. The materials used for awareness measures should ideally support the communication of this content. It is recommended that successful communication be verified through tests.
- The consequences and, if applicable, sanctions for non-compliance with security regulations should be clear from the materials used as part of an awareness measure. At the same time, a user's report of a security breach (e.g. whistleblower) due to their 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. The first step is to determine the needs and then try to plan and implement an awareness campaign tailored to the target group and based on specific potential risks. Information security awareness should not be seen as a one-off project but should be established in the long term via mechanisms planned into the campaign. The effectiveness of a campaign should be analysed in advance. In practice, the following phases have proven to be useful for a security awareness campaign:

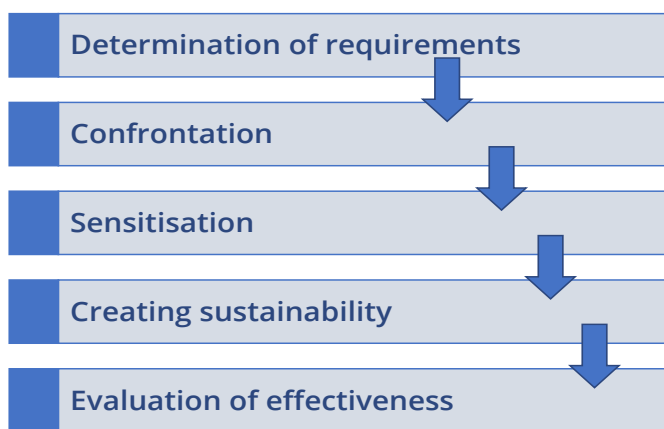


Figure 7: Phase model for security awareness campaigns

Phase 1: Needs assessment (based on hazard potential)

Successful implementation of security awareness campaigns requires that the target groups (stakeholders) and their needs are known. For this reason, awareness campaigns should always start with a needs assessment.

- Security sensitisation makes sense in all areas of the company, but only to an extent that corresponds to the actual risk and the target group.
- Knowledge of security requirements can be demonstrated, for example, through awareness measures with active participation and participant logs.

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

Phase 2: Confrontation with the topic

In the “confrontation” phase, the aim is to raise employees’ awareness of the topic, generate concern and promote acceptance for phase 3, i.e. the actual sensitisation. This is usually best achieved by directly confronting employees with the topic (“experience-based learning”).

- Through their own experience, employees are sensitised to the importance of information security and are usually grateful and open to further training on the subject.

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

- Social engineering attacks on employees, for example with fake calls to obtain confidential information (such as passwords) and fake e-mails (e.g. requesting the password to be entered into an online system with the alleged purpose of checking the password strength for an upcoming audit).
- Provide prepared USB sticks within the company (car park, meeting room, toilets, etc.) that generate warning messages when used, which can be registered anonymously and used for evaluation (“I could have been a virus”).
- Search through wastepaper bins or wastepaper baskets for confidential documents (“dumpster diving”).

Experience has shown that in most companies, the above-mentioned attack scenarios lead to - in this context - “valuable” security incidents and usable information. The “anonymous” resolution of the action in conjunction with the presentation of possible consequences for the company usually ensure a moment of realisation among employees, which can be used as an introduction to the actual IS campaign (“knowledge transfer”). For ethical reasons, it is also advisable to only carry out simulated “attacks” on employees after prior announcement and in close consultation with the works council, if one exists, 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 course. Demonstrations could include live hacking sessions, anonymous password strength checks or role-playing games.

- An essential aspect in this phase is to create a positive entry point for the topic and thus establish contact with the employees “as equals”. Despite all the confrontation, the basic direction must always be to “pick up” the employees where they currently stand (i.e. What IS requirements already exist? How have they been communicated so far? What incidents have already occurred? etc.) and actively involve them.
- It is also important to be aware of the conditions and to recognise any information gaps that may exist. The scope of the activities carried out, and the information provided must be balanced with the “absorption capacity” of the addressees. Only in this way the campaign can develop its full effect and will not be perceived as either too trivial or too excessive/overloaded.

Phase 3: Sensitisation

The actual sensitisation is at best a mix of knowledge transfer, demonstration and active employee participation. Various methods can be used to impart knowledge (classroom training, e-learning, etc.).

The categorisation of awareness-raising measures into subject areas or measures has proven successful:

- Physical safety/workplace safety
 - What must be observed when accessing the buildings and premises?
 - How can unauthorised persons be prevented from gaining access, e.g. incorrect deliveries or an unknown person attaching themselves to a group of employees and entering the building unnoticed (“piggybacking”)?
- Data protection
 - The data protection section should emphasise the legal requirements, e.g. data confidentiality, deletion procedures and employee obligations.
- IT security
 - What should be considered when using IT systems and computers, e.g. handling e-mails, surfing the Internet, handling removable media (CDs, USB sticks), protection and tools against malware?
- Telephone
 - What can happen if sensitive information or processes are disclosed over the phone?
- Reporting and dealing with security incidents
 - What (central) contact points are there?
 - What are relevant initial measures?

In addition, particularly vulnerable target groups (e.g. IT administrators, employees and managers with extensive access and information rights, mobile employees, but also call centre employees or other groups with external contact) must be considered in order to weigh up whether they require special training.

Awareness materials should be created and distributed as required to support the training sessions. 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.).

- Ideally, awareness materials are created by the company’s own employees as part of the IS campaign. Additional motivation for cooperation can be achieved via an incentive system.
- A top management video can emphasise the importance of the topic and encourage employees to handle information with care.

Phase 4: Creating sustainability

One-off awareness measures are not enough to bring about a lasting change in behaviour among employees. Although it is necessary to carry out extensive initial sensitisation, only regular repetition of the topics based on a training plan and regular communication of the key messages in everyday life can ensure lasting awareness. Possibilities for creating an unconscious presence of the topic in everyday life are, for example

- Regular sending of simulated phishing e-mails, e.g. to disclose access data
- Publication of current news (e.g. via the intranet, employee magazine)
- 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 organisation of a cyber security month with e.g. internal or external presentations, live hackings etc.

Phase 5: Evaluation of effectiveness

In this phase, the maturity level of employee sensitisation is assessed at regular intervals. The aim is to create transparency regarding the maturity level of employee sensitisation. Possible KPIs for measurement include, for example

- Number of safety incidents declared due to misconduct in relation to all safety incidents
- Number/ratio of click rates or password entries on simulated phishing emails
- Results of a quiz or test on the topic of information security
- Net Promoter Score (NPS) for training content

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

- Proof of the competency of employees within the scope of the ISMS (Section 7.2)

Furthermore, the following documents have been found to be useful in practice:

- Awareness/training concept
 - What topics are covered?
 - How are awareness measures implemented, e.g. classroom training and/or online training?
 - How is the content of the information security policy communicated?
- Awareness/training programme
 - When are which topics dealt with?
 - Do updates on measures take place regularly, as required by the standard?
- Training documents that succinctly and concisely summarise the contents of the information security guideline and point out dangers and weak points in information processing
- Proof of participation: names of participants, content and date of the awareness programme

References

ISO/IEC 27001:2022 - Sections 7.2 and 7.3

3.11 Supplier Relationships

Increasing interconnection and standardisation in information processing have strongly supported the involvement of external service providers and suppliers. Consequently, security risks at the service provider/supplier also have an impact on the company’s own infrastructure. This is demonstrated by several 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”

According to the understanding 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 more.

The requirements of ISO/IEC 27001:2022 focus on various protective measures, such as the definition of processes and procedures (Annex A.5.19) and the agreement of contractual regulations with the supplier (Annex A.5.20), e.g. connection to logging or security logging, CERT connection, reporting channels for security incidents, integration into existing identity management system. Risks from the supplier’s ICT infrastructure, supply chains and other subcontracting (Annex A.5.21) as

well as regulations for monitoring and changing the provision of services (Annex A.5.22) must also be taken into account.

A topic-specific policy should be established e.g. for the use of cloud services and processes should be developed for the entire life cycle of a service (Annex A.5.23). In this way, relevant aspects of information security are to be addressed from acquisition, use, operation 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 each process. Certification in accordance with 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 relevant standards in this context, divided into overview, requirements and guidelines, as well as supplementary documents focussing on processes and techniques.

In regulated industries, further specific requirements may need to be taken into account. Furthermore, ISO 28001 “Security management systems for the supply chain” is increasingly found as part of customer contracts. This standard also specifies requirements for information security (e.g. physical security, personnel security, IT security).

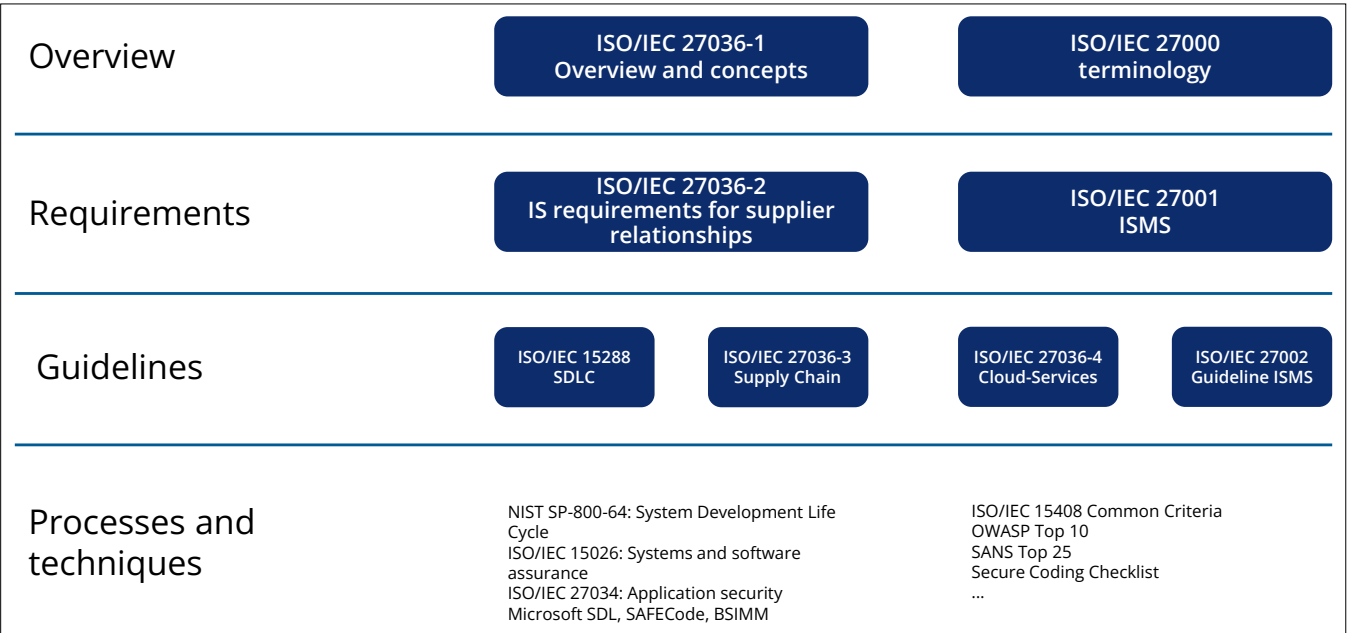


Figure 8: IS standards overview of supplier relationships

Success factors from practice

Holistic risk assessment

It is important to address all risks to which an organisation is exposed through collaboration with external service providers. At this point, the standard demands that all outsourced processes are clearly defined and sustainably managed (see Section 8.1).

ISO/IEC 27036-1 provides a possible categorisation of supplier relationships:

- ▀ Supplier relationships for products
- ▀ Supplier relationships for services
- ▀ Supply chain for information technology
- ▀ Cloud computing

Use of software

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

Right to audit

The right to audit should always be included in every contract.

- ▀ However, this right is not usually granted in standard contracts with cloud providers. In this case, alternatives should be considered, such as access to the results of external audits or the provision of certificates, including the respective scopes.

Certifications

Suppliers are increasingly responding to customers' demands for information security by means of certifications. ISO/IEC 27001:2022 or IT-Grundschutz are particularly suitable for this purpose. However, ISO/IEC 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 Organisation" 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 audit and its results is very important, as the scope of an audit and the controls tested may vary. For critically categorised suppliers, a SOC Type II report in accordance with ISAE 3402 should be requested. Furthermore, potential deviations should be assessed by the client according to their own risk appetite.

- ▀ In the case of personal data, the use of service providers, especially those operating outside the German legal area or outside the EEA²², must be examined critically.
- ▀ This context also includes the topic of commissioned data processing in accordance with Art. 28 EU GDPR regardless of where the service provider is located.

Key figures

The following key figures²³ can be used, for example, to analyse 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 that contractually guarantee IS measures in relation to all service providers.
- ▀ Number of security incidents at service providers in the past reporting period.

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

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

In addition, the following documents have established themselves as useful in practice:

- ▀ Processes and procedures for service provider relationships (see ISO/IEC 27001:2022, A.5.19 - A.5.22). Requirements resulting from the procurement strategy and any service provider relationship should be defined there. Information security risks within the ICT service and product supply chain should also be addressed.
- ▀ Agreements on information security requirements with suppliers. The different categories of suppliers should be considered here.
- ▀ Topic-specific guideline on the use of cloud services (see ISO/IEC 27001:2022, A.5.23).
- ▀ Industry-specific security requirements such as the BDEW white paper from the energy sector.

References

ISO/IEC 27001:2022 - Sections 4.3 and 8.1 as well as 5.19 - 5.23
ISO/IEC 27036-1:2021

²² EEA: European Economic Area.

²³ See also: Evaluation of the performance of an ISMS by key indicators (ISACA Germany Chapter).

BDEW Whitepaper Requirements for secure control and telecommunication systems

VDA - Information Security Assessment

ISAE 3402 - Assurance Reports on Controls at a Service Organisation

3.12 Internal Audit

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

To this end, an audit program must be planned and introduced to regulate aspects such as frequency, procedures, responsibilities and accountabilities, planning requirements, follow-up and reporting. It is also necessary to define how corrective and preventive actions (i.e. actions derived directly from the audits) are to be dealt with, where and by whom they are to be followed up for further processing.

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

Internal audits within the meaning of the standard do not only refer to the activities carried out by the internal audit function

or department. In practice, internal ISMS audits are also a central task of the ISMS manager/CISO, who also 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

A distinction can be made between two areas when implementing internal audits (see Figure 9):

- The “audit program” or “audit framework”, which serves as an organisational superstructure for controlling and monitoring all activities in the context of internal audits and forms the interface to other processes in the ISMS.
- The specific “audit activities”, which include the respective planning and practical implementation of individual internal audits.

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

In larger organisations, an organisational separation between these areas makes sense, whereby an audit team leader is responsible for the audit program, and a team of auditors carries out the internal audit activities. 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 organisation the best possible return on investment (ROI) for the use of resources in the audit area.

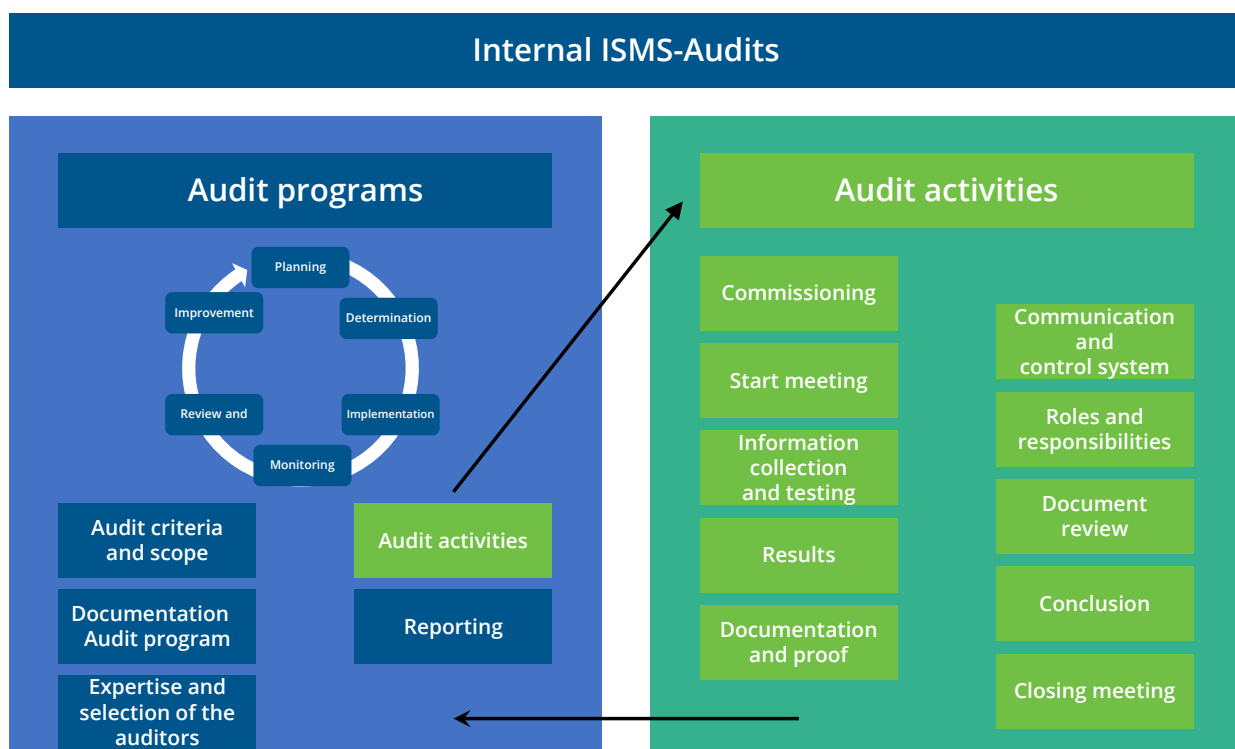


Figure 9: Structure for internal ISMS audits (audit programs vs. audit activities)

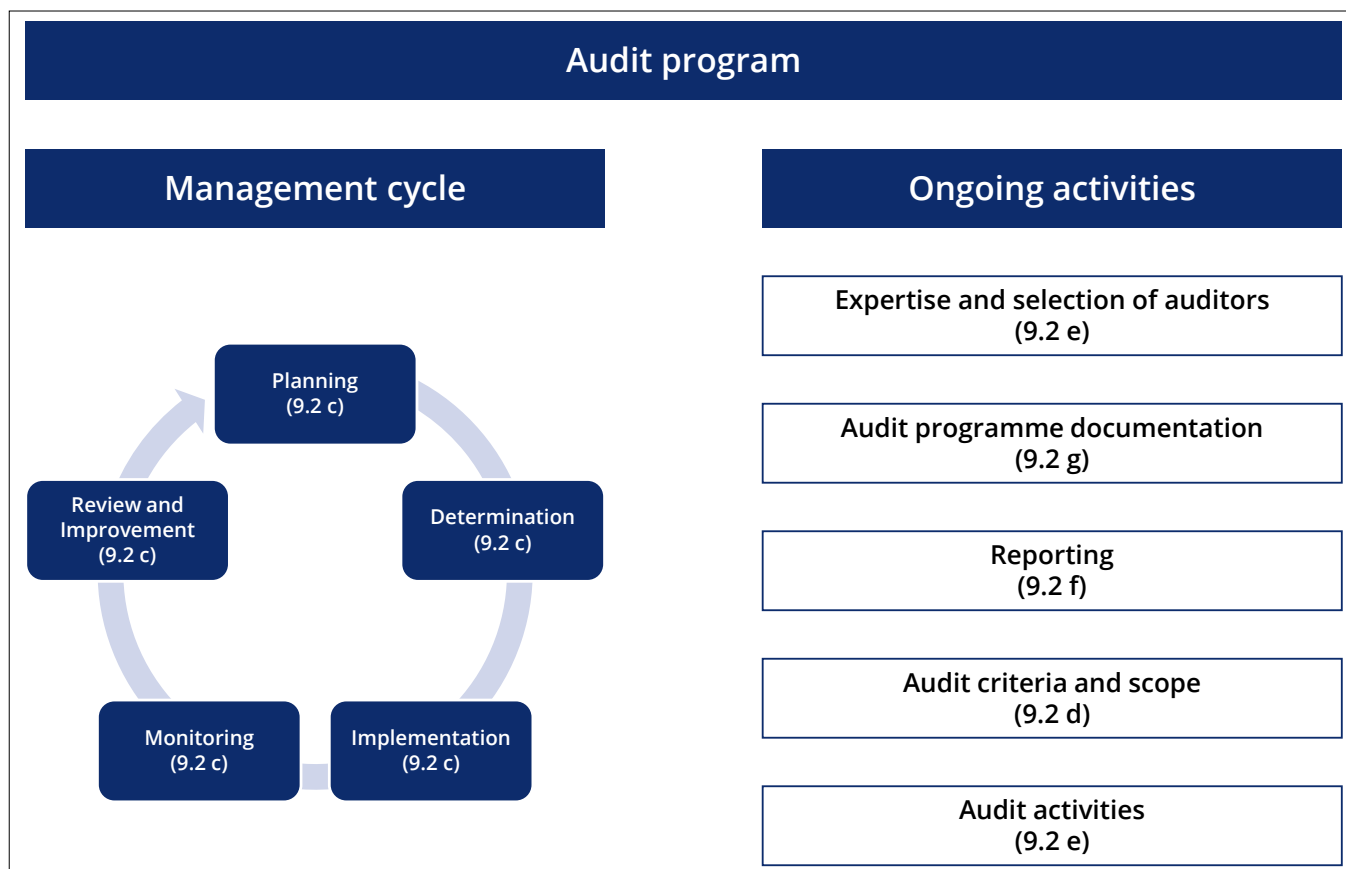


Figure 10: Requirements for the audit program

The audit programme

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

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

Planning sub-process

The audit program should be based on the individual requirements of the respective organisation (see Sections 4.2 and 4.3 of the standard and Chapter 3.1 *Context of the organisation* of this guide). Furthermore, the defined objectives of the audit program should indicate that:

- the audits are orientated towards the risks identified,
- the importance of the individual business processes is considered and
- the audit program covers the scope of the associated ISMS.

Determination sub-process

The employee responsible for the audit program must fulfil the following tasks, among others:

- Definition and implementation of the entire audit program
- Identification, assessment and treatment of risks directly affecting the audit program (e.g. insufficient resources, gaps in auditor qualifications, overly broad scope for individual audits)
- Establishment of processes for conducting audits

24 References in brackets refer to section 9.2 of the ISO/IEC 27001:2022 standard.

- Identification 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 assurance of their qualifications and experience
- Ensuring that audit program documents are always kept up to date
- Ongoing monitoring and improvement of the audit program itself

Implementation sub-process

To implement and execute the audit program, the decisions made during the determination process must be implemented.

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

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

Monitoring sub-process

In the “Monitoring” sub-process, the audit program itself must be continuously monitored in terms of quality and efficiency. Among other things, it must be analysed whether:

- the audit program is still aligned with the scope of the ISMS and the business requirements,
- the time and resource planning are appropriate or adequately designed,
- the “relevant” processes/areas/applications/systems/data are audited and
- the depth and type of testing are suitable to optimally support the objectives.

It is helpful to document the effort required for each audit. As the effort required can vary depending on the characteristics of the IT system and/or the organisational unit concerned, data can be collected in this way in order to better estimate the effort required for future audits.

When monitoring the performance of the audit team members, it is important to pay attention to the quality, e.g. the objectivity, clarity and comprehensibility of the audit results. Among

other things, it is relevant here whether the business department responsible for an IT system has received clear, appropriate and comprehensive recommendations for action in response to the identified deficiencies. If recommendations for actions have not been understood, e.g. because information is missing or recommendations for actions are not appropriate, this is an indication that the members of the audit team require additional technical or methodological support.

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

Review and improvement sub-process

In the “Review and improvement” sub-process, the people responsible for the audit program regularly check whether the expectations of the stakeholders are still being met. The starting point is the information collected in the “Monitoring” sub-process. Furthermore, the continuous professional and methodological development of the auditors must be determined and managed²⁵.

The status of the audit program must be reported to the responsible management. The introduction of KPIs is also useful here in order to make the quality level of the audit program and the internal audits measurable and comparable. Quality statements such as “percentage of measures accepted by departments and initiated for implementation” are to be favoured over pure time statements such as “working time spent per audit”.

Expertise and selection of auditors

- ISMS auditors should be selected in such a way as to ensure the necessary objectivity, expertise and impartiality in the audit process.
- The necessary competencies of an internal auditor should be outlined (e.g. in a role or job description).

Planning and conducting audits

Audits are used to identify non-conformities with existing requirements as well as potential previously unknown weaknesses and hazards.

- The following applies to audit planning: no audit without a dedicated audit assignment. This means that the actual work is only started once the assignment has been secured and formally communicated. In addition, the area to be audited should be actively involved in the audit planning, for example to agree the scope (what will be audited), the time schedule and the availability of contact persons during the audit.

²⁵ See also section 7 of ISO/IEC 19011:2018.

- ▶ Where possible, (immediate) measures for the appropriate handling of hazards should be derived during the audit. However, implementation must be formally agreed with the respective service, system and/or risk owners.
- ▶ If previously unknown process-related deficits or risks are identified that cannot be dealt with in the short term, these must be included in the central risk inventory.
- ▶ Audit results must be reported regularly to the executive level of the ISMS (at least in consolidated form).
- ▶ Audit reports must clearly state which systems and documents were checked or inspected and used as the basis for the audits.
- ▶ Open communication that is maintained throughout the entire duration of an audit makes a significant contribution to reducing reservations in the audited area and thus reduces the risk of information being withheld or not being presented realistically²⁶.
- ▶ In order to determine the suitability, completeness and effectiveness of the measures implemented, the auditor usually directly questions the employees who are primarily responsible for the operation and monitoring of these measures, checks the documentation and/or arranges and assesses practical demonstrations. Auditors are required to have extensive technical knowledge and methodological skills. It is therefore advisable to select the auditors based on the objectives and content of the respective audit.
- ▶ In the context of planning individual audits, i.e. before implementation begins, the responsible management levels must clarify the assumption of the costs incurred.
- ▶ The results should be discussed with the audited area at the latest in the final meeting of an audit, as the audited area should understand and accept the findings and recommended measures. A formal acceptance of the audit report should be sought. Disagreements that cannot be resolved must be documented in the report.
- ▶ It must be ensured that the relevant information and audit reports are treated confidentially and stored or archived in such a way that they are protected against unauthorised 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 8.5 “Performance of internal ISMS audits (process diagram)”, page 69), whereby it should be noted that the normative requirements according to ISO/IEC 27001:2022 are nowhere near as extensive as those described in current best practices.
- ▶ Further information on internal audits can be found, for example, in the ISACA Quality Assurance Review (QAR) guide. Although this guide is focussed on internal IT audits, it can also be used for internal ISMS audits²⁷.

Differentiation between internal ISMS audits and certification audits

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

Certification audits are always external audits. They are carried out by qualified external auditors on behalf of a certification body. External auditors generally work based on the two standards “ISO/IEC 27006-1:2024 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) is a key management and monitoring tool. Aspects of the ISMS can be a component of the internal control system, but the ICS usually goes far beyond the ISMS and primarily includes technical 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 the risk analysis, good management practices or internal and external requirements (e.g. dual control principle for posting approval, multi-factor 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 defence”, which is intended to ensure the correctness of processes and activities in the company and is performed by the direct management level.

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

- ▶ If an ICS has already been established or is currently being set up 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. Complete integration will not be possible in practice, as the objectives of the two systems differ substantially. However, organisational interfaces to the ICS and internal audit are recommended in any case.
- ▶ COSO or COBIT, for example, are used in practice to model an ICS.

26 See also “Communication - The Missing Piece”, ISACA Journal 3/2012 (<https://www.isaca.org/-/media/files/isacadvp/project/isaca/articles/journal/archives/journal-volume-3-2012.pdf>).

27 See https://www.isaca.de/sites/default/files/attachements/isaca_leitfaden_ii_2016_gesamt_screen.pdf.

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

- Documentation of the audit programs (Section 9.2.2)
- Documentation of the audit results (Section 9.2.2)

References

ISO/IEC 27001:2022 - Section 9.2

ISO/IEC 19011:2018

ISO/IEC 27006-1:2024

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-related incidents are usually non-conformities which, if their causes are investigated, have a decisive influence on the continuous improvement process (CIP) and the maturity level of the ISMS. Ultimately, only those who recognise mistakes 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 achieve the best possible long-term benefit from a management system operated within “unpredictable” 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. to define and practise responsibilities, processes and handling options in advance.

The fundamental aim of the process for handling information security incidents is to ensure largely coordinated, targeted and therefore efficient action in the event of an actual security breach or a targeted cyber-attack.

- This chapter solely addresses the topic of “information security incidents”. For the development of a holistic emergency preparedness system, please refer to ISO 22301:2019 “Security and resilience - Business continuity management systems - Requirements”.
- The organisation must define a meaningful categorisation for incidents that enables a practicable and reasonable delimitation of the degree of severity, e.g. differentiation between incidents, security incidents, emergencies and crises.

- A corresponding “Incident Response Plan” should be developed in which the key processes are set out (see Annex A 5.24 in ISO/IEC 27001:2022). Although this cannot cover every particularity, it serves as a guide when an incident occurs and ensures a targeted approach.
- In an emergency, only what has been previously communicated and repeatedly practiced will work. Anyone who relies instead on the fact that the employees affected (which ones are they?) still know “in the event of an emergency” where to look in their treatment plan (where was it filed?) 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 to them, is only slightly better prepared when a real security incident occurs than someone “without a plan” - at least for the first few minutes or hours. However, this is exactly what matters “in the event of an incident”. It is therefore not enough to have the plan in a drawer - it must be known, and the procedure must be practised.
- The process for handling security incidents and its level of detail should consider the organisation’s risk appetite and the conditions of the ISMS.

Planning and preparation

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 organisation and employees for such an event in the best possible way. In addition to generic problem-solving strategies, contact persons and escalation channels in particular must be defined in advance.

Recognising and accepting

- Security incidents should always be reported to a central reporting centre (regardless of the input channel). A defined reporting channel should be offered to all relevant groups where IS incidents may occur, such as employees, IT suppliers, customers and partners.
- Rules of behaviour in the event of safety-related irregularities, including contact points/reporting plans, should be provided in a targeted manner.

Classifying and deciding

- The reporting centre decides whether the reported event is actually a security event or whether it is a non-security-related event, a so-called “known error” (“problem”), for which a solution description already exists, or even an emergency for which an emergency plan may exist. In case of doubt, an escalation (possibly via a “Manager on Duty”) must take place. The reporting centre must be trained accordingly.

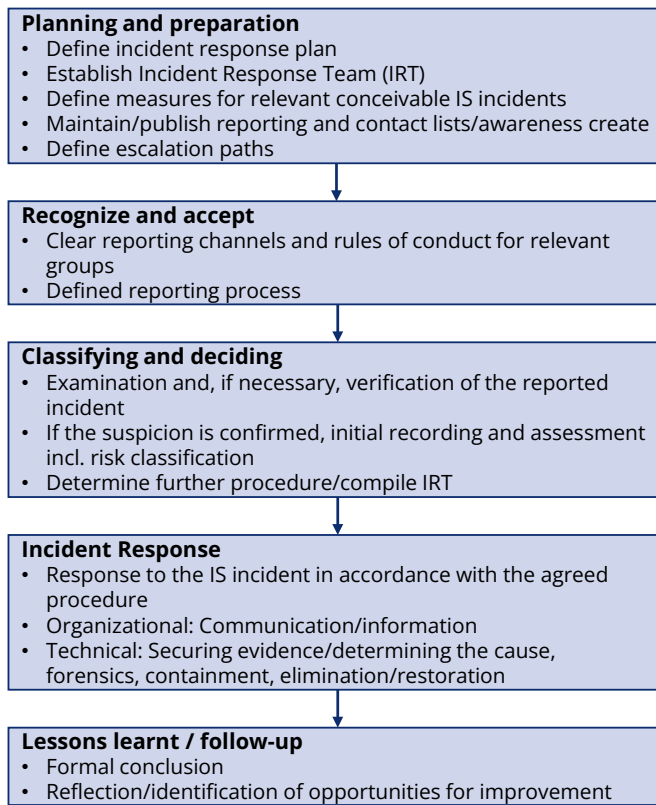


Figure 11: Incident response management - phase model based on ISO/IEC 27035-1:2023

- All incoming incident reports should be documented. As a minimum, the following information should be recorded:

 - Unique identification number
 - Date of acceptance and occurrence of the security incident
 - Name(s) of the reporter(s), name(s) of the data subject(s) and identification(s) of the information/IT systems
 - Description of the security incident (How did the attacker proceed, which vulnerabilities were exploited? Damage caused so far)
 - Any immediate measures already taken
- All security incidents must be classified according to a pre-agreed 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) must be informed.
- The security incidents documented in the (ticket) system should be subject to monitoring, if necessary, to ensure that low-classified incidents are also processed.

Incident Response

In terms of incident response, the following procedure has proven to be 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, through forensic analysis and pre-defined and practised (!) procedures (see also Control 5.28).

Examples of local containment measures:

- Blocking of compromised user accounts
- Shutdown of attacked or jeopardised services
- Use of malware tools (virus scanners, anti-spyware or similar programmes) 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 certain services and/or protocols and selected IP addresses

2. Elimination and restoration: Measures to restore the target state of information/an IT system: In many cases, this can be done by restoring the backup. In this case, the data and software are restored from “clean” data 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, updates and patches must be installed) and the backup files are free from changes made by an attacker.

Another measure can be, for example, updating system software and hardening the affected systems.

3. Root cause identification and (extended) preservation of evidence: Determination of the origin (“root cause”) of the event and securing potential indications and evidence, if necessary, through further forensic analysis.

Lessons learnt/follow-up

- The traceability of a security incident should be ensured at all times. This means that every incident must be visible,

 - the current status of the processing (e.g. New, Accepted, In progress, Paused, Resolved, Completed),
 - who the employees responsible for processing are, if applicable,
 - what measures are (currently) planned to solve the problem,
 - when the implementation of the necessary measures is planned.
- All documented security incidents must be reviewed (after processing) to determine whether better handling of similar incidents can be achieved in future by optimising the “Incident Response Plan” or by making changes to the organisational and operational structure (including the creation or adaptation of instructions).
- The processing of security incidents must always be documented at the end to show how such incidents can be avoided in future or how their impact can be minimised. From this, further measures can be derived, if necessary, which are to be transferred to regular operations.

Documentation requirements

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

In practice, however, the following documents have found to be useful:

- Incident Response Plan (IRP), including up-to-date (!) contact lists and escalation plans
- Code 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 - 5.24 - 28 and 6.8

ISO/IEC 27035-1:2023

ISO/IEC 27035-2:2023

ISO 22301:2019

3.14 Continuous Improvement

Even though many guides and books have been written about the perfect management system, they will probably never exist in practice, as organisations are too diverse to be served with a uniform ‘recipe’. In addition, the environment and the specific conditions are constantly changing, so there can never be a “best solution forever”.

Organisations are therefore called upon to analyse existing best practices and constantly adapt them to their needs. They are required to derive potential for improvement from their non-conformities and thereby continuously improve their ISMS. This process is known as the continuous improvement process (CIP).

An organisation that wishes to operate a standard-compliant ISMS must therefore define organisational measures based on 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 organisation must demonstrate how it ensures that any deficiencies identified are not repeated.

PDCA (Plan-Do-Check-Act) cycle

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

- Plan
 - Establishment of IS goals and responsibilities for achieving them
 - Establishment of the security measures to achieve the IS objectives and the operational process owners for these measures
 - Definition of performance indicators that allow performance measurement against IS targets and associated monitoring measures.
 - Definition of the process for measuring performance including the measuring points, calculation method of the indicator and the standard and tolerance ranges
 - Definition of appropriate immediate and corrective actions when necessary
- Do
 - Continuous measurement of IS target achievement
 - Initiation of corrective action in the event of identified defects or non-conformities
- Check
 - Monitoring of individual safety measure indicators and compare individual performance against IS targets
 - Monitoring of the implementation and effectiveness of the measures introduced.
 - Creation of security reports with key performance indicators for management based on the IS objectives. These reports should contain options for action for necessary management decisions to strengthen the security measures that regularly run into the tolerance range or exceed the threshold for ineffectiveness.
- Act
 - Making the necessary management decisions to restore the effectiveness of security 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 an existing deviation.

Possible sources of deviations and suggestions for improvement

- Conclusions from KPIs - analysis and measurements
- Follow-up of security incidents
- Results of (internal) audits
- Management review and control by the management
- Company suggestion scheme (improvement suggestion)
- Measures derived from the risk treatment

- Measures from the continuous improvement process (CIP) should be included in an overarching implementation plan so that there is a central, consolidated or at least a business unit-wide list of measures.
- Furthermore, regular risk analysis lead to continuous improvement of the ISMS. The results of the risk treatment are an essential part of improving the ISMS, as risk-minimising measures are identified and incorporated into risk treatment plans for implementation.
- The overarching implementation plan facilitates the monitoring of the implementation status and the due date of implementation deadlines as well as the necessary review of the effectiveness of an implemented measure.
- Correction vs. corrective action: If deficiencies and non-conformities are identified, the organisation must react and correct or eliminate them (see Section 10.1 a and b). Corrections are used to rectify or eliminate non-conforming situations. To prevent the recurrence of the same defect, it is necessary to conduct a sustained root cause analysis and define corrective actions (see Section 10.1 c to g).

Documentation requirements

In accordance with ISO/IEC 27001:2022, the following minimum documentation requirements apply:

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

Furthermore, the following documents have been found to be useful in practice:

- Procedure 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 checking 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 Operationalisation of Management Systems

Integration of existing management systems

The previous guideline focuses on the introduction of an ISMS, but only partially considers the often-useful integration of the management system into existing governance structures, including the associated opportunities and challenges, such as the utilisation of synergies by bundling measures or control sets.

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

All management systems have large overlaps in their structure, internal and external requirements and therefore also opportunities to utilise synergies. Harmonised requirements for management systems mean that individual measures can be used across management systems, such as document control or the integrative application of risk assessments. This reduces the effort and risk involved in introducing, operating and verifying the management system.¹

This chapter identifies some of the challenges that frequently recur in companies, as well as useful approaches. It explicitly addresses not only new management systems to be introduced, but also possible potential for improvement of established systems. Due to the immense increase in cybersecurity threats in recent years and the rapidly growing compliance requirements, especially for internationally active organisations, established systems must also ask themselves whether the current regulations / processes are still up to date to meet the growing tasks not only effectively but also efficiently.

For example, enquiries such as the following 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 to have a security self-assessment carried out in accordance with ISO/NIST/BSI/VDA-ISA/EU-GDPR.

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

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

In the meantime, some risk management/compliance/ISMS tool providers have adapted their solutions so that organisations can define specific control objectives, which, in addition, can be linked to the control objectives of the various standards.

This allows to check the degree of maturity or fulfilment of a standard at any time and immediately recognise which controls of the selected standard still have outstanding issues or risks.

Operationalisation through the establishment of a “corporate control database”

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

In most organisations, the managers responsible for a management system currently still define their own measures, which means that many control measures, e.g. secure deletion of information, are maintained twice – if not three or more times – in different places in the organisation, including all follow-up measures, such as implementation status surveys, auditing, effectiveness checks. This inevitably leads to additional work and, in particular, to a lack of understanding on the part of the person responsible for the topics the same questions are asked by various reviewers or auditors.

Those responsible are also affected by industry-, product- and performance-specific norms, standards and best practices, which often contradict each other. Meeting these requirements is made particularly difficult by many different, manual and isolated processes.

The harmonised structure of the 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

¹ See Annex SL

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

that are not directly IT-relevant, such as quality management, occupational health and safety and environmental protection, also follow the new structure and thus enable an organisation-wide integrated management system in the context of GRC.

A corporate control database harmonises rules for the user across various specifications and guidelines based on a common framework. This is also accompanied by a change in approach in which the control measures are no longer based on standards but on topics. The alignment with domains (see below) is expedient for this.

The standards are assigned and maintained with the help of a meta-level. This meta-level thus enables the entire organisation to consolidate existing measures³. The advantage of this is that the answers to other “standards/laws/best practices” that were not previously considered can be seen, even if the new compliance requirement has never been addressed before. At the same time, this enables users to meet individualised industry-, product- or performance-related requirements and monitor compliance.

They also include corresponding workflows and interfaces so that changes can be integrated automatically. This consolidates governance requirements and integrates them into a holistic risk and compliance management system. The quality of the database increases with each new assessment of a standard or norm.

Operationalisation through alignment of the “Central Corporate Controls” with domains

In practice, it has proven useful to group and align the aspects to be managed in the organisation into domains in order to create a clear thematic assignment and responsibility. These domains should be integrated into the overarching model of the organisation in relation to its management systems, with COBIT providing guidance.

Underlying domains from the area of information security could be taken from ISO/IEC 27002, for example. With the new version, the grouping could be based on the new “Cybersecurity Concepts” property, for example. Alternatively, a grouping according to the BSI IT-Grundschutz Compendium or NIST Special Publication 800-53 would be conceivable. It is important that all areas in focus are covered.

The choice of control framework is of secondary importance here and should be selected appropriately by the organisation for its purposes, which can ultimately also vary due to external requirements or the business model. A car manufacturer is more likely to use TISAX, while a SaaS provider is more likely to use the Cloud Control Matrix (CCM) from the Cloud Security Alliance (CSA), for example, while the BSI compendium is particularly useful in highly regulated environments.

Whatever the organisation decides, with appropriate software support or manual diligence, the standard ultimately chosen can be maintained via a meta-level so that many standards can be largely considered. In this approach, the person responsible for the domain is responsible for resolving innovations, conflicts of requirements or ambiguities at a central point. The quality of the database thus increases with each new assessment of a standard.

³ See, for example, the controls from the standards IDW PS 951, EU GDPR (ISO/IEC 27701:2019), ISMS (ISO/IEC 27002:2022), BCMS (ISO 22301:2019), QMS (ISO 9001:2015) through 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 units of a group of companies) in accordance with Art. 28 EU GDPR.

APT Advanced Persistent Threat

Asset Anything that has value for the organisation, also known as an information asset or information value. There are many asset types, such as: Information, software, hardware, services, people and their qualifications, competency and experience as well as intangible assets such as reputation and image. ISO/IEC 27005:2022 distinguishes between primary and secondary assets, with primary assets comprising 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.

BIA Business Impact Analysis

BCMS Business Continuity Management System

BCS Business Criticality Scorecard

BDEW Federal Association of the Energy and Water Industry (Bundesverband der Energie- und Wasserwirtschaft)

BO Business Organisation

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

BSIMM Building Security in Maturity Model

CCM Cloud Control Matrix

CERT Computer Emergency Response Team

CIO Chief Information Officer

CIS Centre for Internet Security

CISO Chief Information Security Officer

COBIT Control Objectives for Information and Related Technology - an internationally recognised framework for IT governance with a focus on IT processes and control objectives.

COSO Committee of Sponsoring Organizations of the Treadway Commission - a US organisation that has developed the recognised standard for internal controls, the so-called COSO model, among other things.

CSA Cloud Security Alliance

DPO Data Protection Officer

GDPR see EU GDPR

EU European Union

EU-GDPR EU General Data Protection Regulation

EEA European Economic Area

IEC International Electrotechnical Commission - an international standardisation organisation that has developed the ISO/IEC 2700x standard together with ISO, among others.

ICS Internal control system

ICT Information and Communications Technologies

IS Information Security

ISAE International Standard on Assurance Engagements

ISMS Information Security Management System - Part of the overall management system, based on a business risk approach, for establishing, implementing, operating, monitoring, reviewing, maintaining and improving information security. The management system includes the organisational structure, policies, planning activities, responsibilities, practices, processes and resources.

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

ISO Information Security Officer

KPI Key Performance Indicator - a performance indicator

KRI Key Risk Indicators

KCI Key Control Indicators

CIP Continuous improvement process

MaRisk Minimum Requirements for Risk Management - an administrative directive on the organisation of risk management in German credit institutions issued by the German Federal Financial Supervisory Authority (BaFin).

NIST National Institute of Standards and Technology

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

OT Operational Technology

OWASP Open Web Application Security Project

QAR-IT ISACA guidelines for conducting a Quality Assurance Review of the internal IT audit (QAR-IT).

QA Quality assurance

QMS Quality Management Systems

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

PII Personally Identifiable Information

RACI matrix Organisations use the RACI categorisation to describe which role is responsible for which activities and which roles are to be involved. This enables a clear description of responsibilities and competencies. The terms are interpreted as follows:

- ▀ *Responsible* - responsible for the actual implementation (*implementation responsibility*). The person who gives the initiative for implementation to others. Also interpreted as responsibility in a disciplinary and qualitative sense.
- ▀ *Accountable* - accountable (*overall responsibility*), responsible in the sense of “authorising”, “approving” or “signing”. The person who bears responsibility in the legal or commercial sense. Also interpreted as responsibility from a cost centre perspective.
- ▀ *Consulted* - consulted (*professional expertise*). A person whose advice should or must be sought. Also interpreted as responsibility from a professional perspective.
- ▀ *Informed* - to inform (*right to information*). A person who receives information about the progress or outcome of the activity or is authorised to receive information.
- ▀ As a rule, only one person (role) should be *accountable* for each activity. However, several people can be *responsible*, *consulted* or *informed* for an activity. It is also possible for one person to be both *accountable* and *responsible* for an activity.

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 of application

SIRP Security Incident Response Process

SLA Service Level Agreement - agreement between client and service provider

SMART Specific, measurable, accepted, realistic, time-bound

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

SOC System and Organization Controls

SoD matrix Segregation of Duties matrix - overview of the segregation of duties between roles within the organisation.

TISAX Trusted Information Security Assessment Exchange

TMG German Telemedia Act (Telemediengesetz)

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

VDA German Association of the Automotive Industry (Verband der Automobilindustrie)

Zero-day vulnerability A previously unpublished 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 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 27006-1:2024 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 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 27014:2020 Information security, cybersecurity, and privacy protection - Governance of information security

ISO/IEC 27032:2012 Information technology - Security techniques - Guidelines for Internet security

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 27036-3:2023 Cybersecurity - Supplier relationships - Part 3: Guidelines for hardware, software and services 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 27017:2015 Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services

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

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 auditing and certification of management systems - Part 2: Competency requirements for auditing and certification of environmental management systems

Further 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 Methodology, version 1.0, 2017

BSI Standard 200-3, Risk analysis on the basis of IT-Grundschutz, Version 1.0, 2017

IT-Grundschutz Compendium 2022, BSI, 2022

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

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

ISACA - Evaluation of the performance of an ISMS through key indicators

Weblinks

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 illustrations

Figures

Figure 1: Integration of the ISMS into corporate management	6
Figure 2: Building blocks of an ISMS according to ISO/IEC 27001:2022	7
Figure 3: Risk management process according to ISO 31000	17
Figure 4: Risk treatment options according to ISO/IEC 27005	18
Figure 5: Structure and relationship of KPI, KRI and KCI	20
Figure 6: Development of a communication plan	23
Figure 7: Phase model for security awareness campaigns	25
Figure 8: IS standards overview of supplier relationships	27
Figure 9: Structure for internal ISMS audits (audit programme vs. audit activities)	29
Figure 10: Requirements for the audit programme	30
Figure 11: Incident response management - phase model based on ISO/IEC 27035-1:2023	34
Figure 12: Scenario-based determination of the risk level	52

Tables

Table 1: Communication plan – Internal communication	24
Table 2: Communication plan – External communication	24
Table 3: Cost of safety analysis	52

8 Appendix

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

The following table shows the conformity 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	Organisational 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	Legal, statutory, regulatory, and contractual requirements	A.18.1.1, A.18.1.5
5.32	Intellectual property rights	A.18.1.2



5	Organisational controls (continued)	
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, rules 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	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
8.11	Data masking	New
8.12	Data leakage prevention	New
8.13	Information backup	A.12.3.1



8	Organisational controls (continued)	
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 synchronisation	A.12.4.4
8.18	Use of privileged utility programmes	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 of 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 conformity 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	Organisation 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



Mapping: ISO/IEC 27001:2013 vs. ISO/IEC 27001:2022 (continued)		
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 on 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.9.3.1	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

Mapping: ISO/IEC 27001:2013 vs. ISO/IEC 27001:2022 (continued)		
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 synchronisation	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

The third edition of ISO/IEC 27001 was published in October 2022. Like other ISO/IEC standards that describe the requirements for a management system (e.g. ISO 9001, ISO 14001, ISO 22301), ISO/IEC 27001 also follows a uniform structure, the so-called “*Harmonised Structure*” of Annex SL of ISO/IEC Directives, Part 1. As this structure changed in 2021, the main chapters of ISO/IEC 27001:2022 were adapted accordingly. The following changes have been made to the main chapters:

- In addition to defining relevant requirements from interested parties, the organisation (Chapter 4, “*Context of the organisation*”) must now also define which of these requirements are addressed by the ISMS (Section 4.2, c).
- Management of changes (Chapter 6, “*Planning*”) has been expanded in 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 has also been expanded with section 6.3 “*Planning of changes*” for the implementation of planned changes to the ISMS. The circumstances that necessitate 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 implementing the processes from Chapter 6 “*Planning*” must be established and 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*” have been divided into further subsections, although their content remains identical.
- Section 9.3 “*Management review*” has been divided into three subsections. It has been added that management reviews must now also cover changes to the needs and expectations of interested parties that are relevant to the ISMS (Section 9.3.2 “*Management review inputs*”, c)).
- Continuous improvement: Chapter 10 has been reorganised so that the statement to continuously improve the suitability, adequacy and effectiveness of the ISMS is placed before the section on non-conformity, with the aim of encouraging improvement rather than corrective action.
- The new version of ISO/IEC 27001:2022 essentially contains a complete replacement of Annex A, which 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”, so the controls are formulated as mandatory here, whereas ISO/IEC 27002 uses the word “should”, so the requirements here are to be understood as recommendations.
- The controls listed in the Annex A still do not claim to be exhaustive and additional measures may be required. As before, companies are also free to use the measures from other sources (e.g. NIST Cybersecurity Framework, BSI IT-Grundschutz, ISF Standard of Good Practice, etc.) to minimise their information security risks. In this case, only a declaration of applicability is required, which contains a mapping of the selected measures to the controls of the annex of ISO/IEC 27001:2022 and the necessary reasons for selection. This confirms that no requirements have been neglected that are actually applicable and necessary to mitigate existing risks (see ISO/IEC 27001:2022, section 6.1.3 “*Information security risk treatment*”, b) and note 2 of section 6.1.3; c) has been slightly amended to make this aspect even clearer).

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

In the new version of ISO/IEC 27002:2022, the change of **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” has been removed to better reflect its purpose as a reference work for information security measures. In addition to the word “Information Security”, the terms “Cyber Security” and “Privacy Protection” are emphasised. As a result, the new version explicitly addresses cyber security measures as a subset of information security measures and privacy protection measures.

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

A new 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. Instead of 14 chapters/domains (“Security Control Clauses”), the new version now contains 4 topics (see below for more details). Directly downstream of this are the 93 measures (“Controls”). This means that the original integration into “control objectives” is no longer applicable for the time being. In future, this will be presented as a purpose for each measure. Overall, measures in the new version include the following content:

- a brief 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 (“*Guidance*”) and
- explanatory text or references to other related documents (“*Other Information*”).

As already 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, if physical objects are affected, e.g. access control;
- “**Technological controls**”, Chapter 8, if the technology is affected and
- All other measures are allocated to “**Organisational controls**”, Chapter 5.

A helpful addition in the new version are the attributes (“*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 categorised, and the measures can be easily filtered.

The reorganisation at measure level has the following effects: In the new version, 11 new controls were added, one control was split, 57 controls were summarised in 24 controls, and 58 controls were reformulated.

The new version therefore contains 93 measures/controls in 4 topics compared to 114 measures/controls in 14 security control clauses in the old version.

New measures

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

- “*Threat intelligence*” (Section 5.7) is definitely new in this form. It involves, among other things, the collection and evaluation of information on the specific threat environment of the organisation in order to be able to take suitable reactive measures: a distinction is made between strategic, tactical and operational threat intelligence.
- “*Information security for use of cloud services*” (Section 5.23), this measure was implicitly anchored in Supplier Relationships in the 2013 version. The measure covers the information security of cloud services from the customer’s perspective. For example, a policy 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 analysis (BIA) is described as a basis.
- “*Data masking*” (Section 8.11) not only deals with the topic of masking (personal) data, but also addresses the properties of pseudonymisation and anonymisation of data, among other things, and legal aspects are also addressed.
- “*Data leakage prevention*” (Section 8.12) extends the original requirement for information classification 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 independent measures in the new standard:

The content of the “*Technical compliance review*” measure (old version, Security Control Clause 18.2.3) is divided into the organisational part “*Compliance with policies and standards for information security*” (Section 5.36), including explanations on checking compliance with the guidelines. On the other hand, there is the technical part “*Management of technical vulnerabilities*” (Section 8.8), which has been greatly expanded and is presented in detail. It deals extensively with the identification and evaluation of technical vulnerabilities and explicitly recommends carrying out pentests, for example.

Summarised measures

A total of 57 measures were summarised in 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 merged from 2 original domains/security control clauses. On the one hand from the measure with the same name “*Information security in project management*” (old version, Security Control Clause 6.1.5), on the other hand the content from “*Information security requirements analysis and specification*” (old version, Security Control Clause 14.1.1) was also included.
- “*User endpoint devices*” (Section 8.1) was also merged from 2 original domains/security control clauses. On the one hand from the measure “*Mobile device policy*” (old version, Security Control Clause 6.2.1), on the other hand the content from “*Unattended user equipment*” (old version, Security Control Clause 11.2.8) has also been incorporated. This brings together all aspects that need to be considered when protecting end devices for users.

Valuation

With the new version, a clear further development and an update regarding recognised information security measures is recognisable, as the standard also promises in the introduction. Important best practices and trends in the information security industry have been considered in the new version, although with 11 new measures, no massive thematic expansions have been made.

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

These and other formal additions can be used to create a variety of views on different aspects. These options and the higher level of detail can simplify the creation of company-related guidelines.

Outlook

The updating of other existing norms and standards in 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.

Organisations already have the option of using the new Annex A measures as measures. These mapping tables can also be used to create declarations of applicability for certified organisations that 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 the certification is still to be carried out explicitly in accordance with the 2013 version. This could be necessary, for example, if the certification body does not yet have accreditation for certification according to the 2022 version. The document "Transition Requirements for ISO/IEC 27001:2022" of the International Accreditation Forum¹ 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 a three-year transition period (by 31 October 2025 at the latest). Thanks to the mappings provided, the effort for such an adaptation should essentially be able to focus on the new measures and on improvements to existing measures of the standard.

Certification bodies must start certifying to the new standard by 31 October 2023 at the latest.

8.3 Holistic safeguarding of the value chain

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

In practice, a "Business Criticality Scorecard (BCS)" has been established for this purpose, which is used to document a classification of the basic risk level of the process or the applications used in it, for example, based on scenarios.

For end-to-end protection, it is useful for the organisation to assess the criticality of the process, and the protection requirements of the information processed in it in a scorecard based on a policy, at least for each main process and for each application operated for the process by the respective process owner.

In addition, it is important that an organisation'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 prioritisation of the business processes to be protected

The scorecard for business criticality is used to carry out a high-level identification of the information security risks resulting from the process or the applications to determine the effort required to secure the asset under consideration. Identification based on organisation-specific fundamental questions and scenarios in the context of the information security objectives, which are shown below as examples (Figure 14), is suitable here.

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

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

For less critical systems, for example, a standard safeguard to be defined can then be applied, and for processes with a higher risk potential, specific security concepts or technical checks, such as the performance of a penetration test, are required. The possible decision levels could be defined as shown in Figure 15 as an example.

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

Level	Safety analysis effort
0	No further analysis necessary
1	Standard measures Carrying out a GAP analysis on the organisation's standard measures or alternatively, if operated by the Group's own IT department, confirmation from the IT department that the measures have been implemented.
2	Extended safety analysis Carrying out a specific vulnerability analysis using threat modelling (e.g. STRIDE) ²
3	Technical safety analysis Performance of a penetration test or source code analysis by an independent third party.

Table 3: Cost of safety analysis

The BCS thus represents a kind of “pre-filter” for risk management, as extensive analysis only need to be carried out if the initial assessment of criticality identifies a corresponding need, but the methodology still ensures that each process is at least analysed at a high level and that an appropriate basic safeguard is guaranteed, which automatically leads to a systematically ensured “weakest link” safeguard.

² See section 3.6

Scenario: Imagine that a hacker (and/or a competitor) would have access to the data/information of the process? [Confidentiality]	How do you assess the risk for OUR ORGANISATION? W S Risk Level Select an element. Select an element. Select an element. Describe the specific damage that would be conceivable for OUR ORGANISATION.
Scenario: Imagine that a hacker (and/or a competitor) could falsify the data/information of the service ("loss of integrity"). [Integrity]	How do you assess the risk for OUR ORGANISATION? W S Risk Level Select an element. Select an element. Select an element. Describe the specific damage that would be conceivable for OUR ORGANISATION.
Scenario: Imagine that the service or the data would not be available for longer than one day [Availability]	How do you assess the risk for OUR ORGANISATION? W S Risk Level Select an element. Select an element. Select an element. Would there be a workaround to fulfil the business requirements (e.g. manual process)? At what point would an outage be critical for OUR ORGANISATION? Select an element.

Figure 12: Scenario-based determination of the risk level

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

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

8.5 Carrying out internal ISMS audits (process diagram)

