International Standard

ISO/IEC 27006-1

Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems —

Part 1: **General**

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information —

Partie 1: Généralités

First edition
2024-03

Reference number
ISO/IEC 27006-1:2024(en)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13 *Cybersecurity and data protection,* in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This first edition of ISO/IEC 27006-1 cancels and replaces ISO/IEC 27006:2015, which has been technically revised. It also incorporates the Amendment ISO/IEC 27006:2015/Amd 1:2020.

The main changes are as follows:

— this document has been converted into the first part of a multi-part series;

— the entire document has been updated for remote audits and organizations with few or no physical relevant sites;

— the concept of persons performing certain identical activities has been introduced in C.3.4 and several updates were provided;

— this document (in particular, Annex E) has been aligned with ISO/IEC 27001:2022 and ISO/IEC 27002:2022;

— redundancies with ISO/IEC 17021-1 have been removed;

— wording has been clarified and more closely aligned with ISO/IEC 17021-1.

A list of all parts in the ISO/IEC 27006 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

ISO/IEC 17021-1 sets out requirements and guidance for bodies providing audit and certification of management systems. If such bodies intend to be compliant with ISO/IEC 17021-1 with the objective of auditing and certifying information security management systems (ISMS) in accordance with ISO/IEC 27001, some additional requirements and guidance to ISO/IEC 17021-1 are critical. These are provided by this document.

This document specifies requirements for bodies providing audit and certification of an ISMS. It gives generic requirements for such bodies which are referred to as certification bodies. Observance of these requirements is intended to ensure that certification bodies operate ISMS certification in a competent, consistent and impartial manner, thereby facilitating the recognition of such bodies and the acceptance of their certifications on a national and international basis.

The text in this document follows the structure of ISO/IEC 17021-1:2015.

In this document, the following verbal forms are used:

— “shall” indicates a requirement;

— “should” indicates a recommendation;

— “may” indicates a permission;

— “can” indicates a possibility or a capability.

Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems —

Part 1: **General**

1 Scope

This document specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021-1.

The requirements contained in this document are demonstrated in terms of competence and reliability by bodies providing ISMS certification. The guidance contained in this document provides additional interpretation of these requirements for bodies providing ISMS certification.

NOTE This document can be used as a criteria document for accreditation, peer assessment or other audit processes.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 17021-1 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
certification document
document indicating that a client's information security management system (ISMS) conforms to specified ISMS standards and any supplementary documentation required under the management system

Note 1 to entry: This definition does not limit the number of documents collectively known as certification documents.

3.2
control
measure that maintains and/or modifies *risk* (3.10)

Note 1 to entry: Controls include, but are not limited to, any process, policy, device, practice or other conditions and/or actions which maintain and/or modify *risk* (3.10).

Note 2 to entry: Controls may not always exert the intended or assumed modifying effect.

[SOURCE: ISO/IEC 27002:2022, 3.1.8]

3.3
external context
external environment in which the *organization* (3.9) seeks to achieve its objectives

Note 1 to entry: External context can include the following:

- the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local;
- key drivers and trends having impact on the objectives of the *organization* (3.9);
- relationships with, and perceptions and values of, external stakeholders.

[SOURCE: ISO/IEC 27000:2018, 3.22]

3.4
information security
preservation of confidentiality, integrity and availability of information

Note 1 to entry: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

[SOURCE: ISO/IEC 27000:2018, 3.28]

3.5
information security incident
single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening *information security* (3.4)

[SOURCE: ISO/IEC 27000:2018, 3.31]

3.6
information system
set of applications, services, information technology assets, or other information-handling components

[SOURCE: ISO/IEC 27000:2018, 3.35]

3.7
internal context
internal environment in which the *organization* (3.9) seeks to achieve its objectives

Note 1 to entry: Internal context can include:

- governance, organizational structure, roles and accountabilities;
- policies, objectives, and the strategies that are in place to achieve them;
- the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies);
- *information systems* (3.6), information flows and decision-making processes (both formal and informal);
- relationships with, and perceptions and values of, internal stakeholders;
- the *organization's* (3.9) culture;

- standards, guidelines and models adopted by the *organization* (3.9);
- form and extent of contractual relationships.

[SOURCE: ISO/IEC 27000:2018, 3.38]

3.8
management system
set of interrelated or interacting elements of an *organization* (3.9) to establish policies and objectives, and processes to achieve those objectives

Note 1 to entry: A management system can address a single discipline or several disciplines, e.g. quality management, financial management or environmental management.

Note 2 to entry: The management system elements establish the *organization's* (3.9) structure, roles and responsibilities, planning, operation, policies, practices, rules, beliefs, objectives and processes to achieve those objectives.

Note 3 to entry: The scope of a management system can include the whole of the *organization* (3.9), specific and identified functions of the *organization* (3.9), specific and identified sections of the *organization* (3.9), or one or more functions across a group of *organizations* (3.9).

Note 4 to entry: This constitutes one of the common terms and core definitions for ISO management system standards given in Annex SL of the Consolidated ISO Supplement to the ISO/IEC Directives, Part 1. The original definition has been modified by modifying Notes 1 to 3 to entry.

[SOURCE: ISO 9000:2015, 3.5.3]

3.9
organization
person or group of people that has its own functions with responsibilities, authorities and relationships to achieve its objectives

Note 1 to entry: The concept of organization includes but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

[SOURCE: ISO/IEC 27000:2018, 3.50]

3.10
risk
effect of uncertainty on objectives

Note 1 to entry: An effect is a deviation from the expected — positive or negative.

Note 2 to entry: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3 to entry: Risk is often characterized by reference to potential "events" (as defined in ISO Guide 73:2009, 3.5.1.3) and "consequences" (as defined in ISO Guide 73:2009, 3.6.1.3), or a combination of these.

Note 4 to entry: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" (as defined in ISO Guide 73:2009, 3.6.1.1) of occurrence.

Note 5 to entry: In the context of information security management systems, information security risks can be expressed as an effect of uncertainty on information security objectives.

Note 6 to entry: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an *organization* (3.9).

[SOURCE: ISO/IEC 27000:2018, 3.61]

3.11
risk analysis
process to comprehend the nature of *risk* (3.10) and to determine the level of risk

Note 1 to entry: Risk analysis provides the basis for risk evaluation and decisions about *risk treatment* (3.14).

Note 2 to entry: Risk analysis includes risk estimation.

[SOURCE: ISO/IEC 27000:2018, 3.63]

3.12
risk assessment
overall process of risk identification, *risk analysis* (3.11) and risk evaluation

[SOURCE: ISO/IEC 27000:2018, 3.64]

3.13
risk management
coordinated activities to direct and control an *organization* (3.9) with regard to *risk* (3.10)

[SOURCE: ISO/IEC 27000:2018, 3.69]

3.14
risk treatment
process to modify *risk* (3.10)

Note 1 to entry: Risk treatment can involve:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing);
- retaining the risk by informed choice.

Note 2 to entry: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention” and “risk reduction”.

Note 3 to entry: Risk treatment can create new risks or modify existing *risks* (3.10).

[SOURCE: ISO/IEC 27000:2018, 3.72]

3.15
rule
accepted principle or instruction that states the *organization’s* (3.9) expectations on what is required to be done, what is allowed or not allowed

[SOURCE: ISO/IEC 27002:2022, 3.1.32 — modified, note 1 to entry has been removed.]

4 Principles

The principles from ISO/IEC 17021-1:2015, Clause 4 shall apply.

5 General requirements

5.1 Legal and contractual matters

The requirements of ISO/IEC 17021-1:2015, 5.1 shall apply.

5.2 Management of impartiality

5.2.1 General

The requirements of ISO/IEC 17021-1:2015, 5.2 shall apply. In addition, the requirements and guidance in 5.2.2 shall apply.

5.2.2 Conflicts of interest

Certification bodies may add value during certification and surveillance audits (e.g. by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions) without it being considered as consultancy or having a potential conflict of interest.

The certification body shall not provide internal information security reviews of the client's ISMS subject to certification. Furthermore, the certification body shall be independent from the body or bodies (including any individuals) which provide the internal ISMS audit.

5.3 Liability and financing

The requirements of ISO/IEC 17021-1:2015, 5.3 shall apply.

6 Structural requirements

The requirements of ISO/IEC 17021-1:2015, Clause 6 shall apply.

7 Resource requirements

7.1 Competence of personnel

7.1.1 General

The requirements of ISO/IEC 17021-1:2015, 7.1 shall apply. In addition, the requirements and guidance in 7.1.2 and 7.1.3 shall apply.

7.1.2 Generic competence requirements

The certification body shall define the competence requirements for each certification function as referenced in ISO/IEC 17021-1:2015, Table A.1. The certification body shall take into account all the requirements specified in ISO/IEC 17021-1, and 7.1.3 and 7.2.2 of this document, that are relevant for the ISMS technical areas as determined by the certification body. Annex B provides further guides on competence.

The certification body shall define the knowledge and skills that are required for certain functions in accordance with Annex A.

Where additional specific criteria including competence requirements have been established in a specific standard, (e.g. ISO/IEC 27006-2), these shall be applied.

7.1.3 Determination of competence criteria

7.1.3.1 Competence requirements for ISMS auditing

7.1.3.1.1 General requirements

The certification body shall have criteria for verifying the competence of audit team members to ensure that they have at least the skills to apply their knowledge of:

a) information security;

b) the technical aspects of the activity to be audited;

c) management systems;

d) the principles of auditing;

NOTE Further information on the principles of auditing can be found in ISO 19011.

e) ISMS monitoring, measurement, analysis and evaluation.

The above requirements a) to e) apply to all auditors in the audit team. However, b) can be shared among members in the audit team.

The audit team members shall, collectively, have skills appropriate to the requirements above, which can be demonstrated through experience of their application.

The audit team members shall, collectively, be competent in tracing indications of information security incidents in the client's ISMS back to the appropriate elements of the ISMS.

Individual auditors are not required to have a complete range of experience of all areas of information security, but the audit team as a whole shall have appropriate competence to cover the ISMS scope being audited.

7.1.3.1.2 Information security management terminology, principles, practices and techniques

Each auditor in an ISMS audit team shall have knowledge of:

a) ISMS specific documentation structures, hierarchy and interrelationships;

b) information security risk assessment and risk management;

c) processes applicable to ISMS.

The audit team members shall, collectively, have knowledge of:

d) information security management related tools, methods, techniques and their application;

e) the current technology where information security can be relevant or an issue.

7.1.3.1.3 Information security management system standards and normative documents

Each auditor in an ISMS audit team shall have knowledge of all requirements contained in ISO/IEC 27001.

The audit team members shall, collectively, have knowledge of all controls contained in ISO/IEC 27001:2022, Annex A and their implementation.

7.1.3.1.4 Business management practices

Each auditor in an ISMS audit team shall have knowledge of:

a) industry information security good practices and information security procedures;

b) policies and business requirements for information security;

c) general business management concepts, practices and the interrelationship between policy, objectives and results;

d) management processes and related terminology.

NOTE These processes also include human resources management, internal and external communication and other relevant support processes.

7.1.3.1.5 Client business sector

Each auditor in an ISMS audit team shall have knowledge of:

a) the legal and regulatory requirements in the particular information security field, geography and jurisdiction(s);

   NOTE Knowledge of legal and regulatory requirements does not imply a profound legal background.

b) information security risks related to business sector;

c) generic terminology, processes and technologies related to the client business sector;

d) the relevant business sector practices.

The criterion a) may be shared among the audit team.

7.1.3.1.6 Client products, processes and organization

The audit team members shall, collectively, have knowledge of:

a) the impact of organization type, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing;

b) complex operations in a broad perspective;

c) legal and regulatory requirements applicable to the product or service.

7.1.3.2 Competence requirements for conducting the application review

7.1.3.2.1 Client business sector

The personnel conducting the application review to: determine the audit team competence required, select the audit team members and determine the audit time, shall have knowledge of generic terminology, processes, technologies and risks related to the client business sector.

7.1.3.2.2 Client products, processes and organization

The personnel conducting the application review to: determine the audit team competence required, select the audit team members and determine the audit time, shall have knowledge of the impact of client products, processes, organization types, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including externally provided functions.

7.1.3.3 Competence requirements for reviewing audit reports and making certification decisions

7.1.3.3.1 General

The personnel reviewing audit reports and making certification decisions shall have knowledge that enables them to verify the appropriateness of the scope of certification as well as changes to the scope and their impact on the effectiveness of the audit, in particular the continuing validity of the identification of interfaces and dependencies and the associated risks.

Additionally, personnel reviewing audit reports and making the certification decisions shall have knowledge of:

a) management systems in general;

b) audit processes and procedures.

7.1.3.3.2 Information security management terminology, principles, practices and techniques

The personnel reviewing audit reports and making certification decisions shall have knowledge of:

a) the items listed in 7.1.3.1.2 a), b) and c);

b) legal and regulatory requirements relevant to information security.

7.1.3.3.3 Client business sector

The personnel reviewing audit reports and making certification decisions shall have knowledge of generic terminology and risks related to the relevant business sector practices.

7.1.3.3.4 Client products, processes and organization

The personnel reviewing audit reports and making certification decisions shall have knowledge of client products, processes, organization types, size, governance, structure, functions and relationships.

7.2 Personnel involved in the certification activities

7.2.1 General

The requirements of ISO/IEC 17021-1:2015, 7.2 shall apply. In addition, the requirements and guidance in 7.2.2 shall apply.

7.2.2 Demonstration of auditor knowledge and experience

7.2.2.1 General considerations

The certification body shall demonstrate that each auditor has knowledge and experience through each of the following:

a) recognized ISMS-specific qualifications;

b) registration as auditor where applicable;

c) participation in ISMS training courses and attainment of relevant personal qualifications;

d) up-to-date professional development records;

e) ISMS audits witnessed by another ISMS auditor.

7.2.2.2 Selecting auditors

In addition to 7.1.3.1, the process for selecting auditors shall ensure that each auditor:

a) has professional education or training equivalent to university level;

b) has practical workplace experience in information technology and information security, which is sufficient to act as auditor for ISMS;

c) has received sufficient training regarding ISMS auditing, and demonstrated skills of auditing an ISMS according to ISO/IEC 27001. This experience shall be gained by performing as an auditor-in-training monitored by an ISMS evaluator (see ISO/IEC 17021-1:2015, 9.2.2.1.4) in at least one ISMS initial certification audit (stage 1 and stage 2) or re-certification and at least one surveillance audit. This experience shall be gained in at least 10 ISMS on-site audits days and performed in the last five years. The participation shall include document review; review of risk assessment and its implementation, and audit reporting;

d) maintains relevant and current knowledge and skills in information security and auditing.

NOTE 1 Skills maintenance can be demonstrated through continual professional development.

NOTE 2 The certification body requires a competence criteria catalogue to match the above requirements and evidences (see ISO/IEC 17021-1:2015, 7.1.2.).

7.2.2.3 Selecting technical experts

The process for selecting technical experts shall ensure that each technical expert:

a) has professional education or training equivalent to university level;

b) has practical workplace experience in information technology and information security sufficient to act as a technical expert;

c) maintains relevant and current knowledge and skills in information security.

NOTE Skills maintenance can be demonstrated through continual professional development.

7.2.2.4 Selecting auditors for leading the team

In addition to 7.2.2.2, the criteria for selecting an auditor for leading the team shall ensure that the auditor has actively participated in all stages of at least three ISMS audits. The participation shall include initial scoping and planning, document review, review of risk assessment and its implementation, and formal audit reporting.

7.3 Use of individual external auditors and external technical experts

The requirements of ISO/IEC 17021-1:2015, 7.3 shall apply.

7.4 Personnel records

The requirements of ISO/IEC 17021-1:2015, 7.4 shall apply.

7.5 Outsourcing

The requirements of ISO/IEC 17021-1:2015, 7.5 shall apply.

8 Information requirements

8.1 Public information

The requirements of ISO/IEC 17021-1:2015, 8.1 shall apply.

8.2 Certification documents

8.2.1 General

The requirements of ISO/IEC 17021-1:2015, 8.2 shall apply. In addition, the requirements and guidance in 8.2.2 and 8.2.3 shall apply.

8.2.2 ISMS Certification documents

Certification documents shall be signed by an officer who has been assigned that responsibility. The version of the Statement of Applicability shall be included in the certification documents.

NOTE A change to the Statement of Applicability which does not change the coverage of the controls in the scope of certification does not require an update of the certification documents.

Where no activity of the organization within the scope of the certification is undertaken at a defined physical location at all, the certification document(s) shall state that all activities of the organization are conducted remotely.

8.2.3 Reference of other standards in the ISMS certification documents

The certification documents may reference national and international standards only if:

a) the organization has compared all of its necessary controls with those in the reference control source(s), to determine that it has not inadvertently omitted any such reference control in accordance with ISO/IEC 27001:2022, 6.1.3 c);

b) a justification for excluded reference controls is stated in the Statement of Applicability (SoA) in accordance with ISO/IEC 27001:2022, 6.1.3 d).

The reference control standards can be based on ISO/IEC 27001:2022, Annex A, or be standards that include information security controls.

The certification documents shall state that the control set(s) applied in the SoA is used only for referencing the relevance of the inclusion or exclusion of controls in the ISMS and not used for conformity assessment.

8.3 Reference to certification and use of marks

The requirements of ISO/IEC 17021-1:2015, 8.3 shall apply.

8.4 Confidentiality

8.4.1 General

The requirements of ISO/IEC 17021-1:2015, 8.4 shall apply. In addition, the requirements and guidance in 8.4.2 shall apply.

8.4.2 Access to organizational records

Before the certification audit, the certification body shall ask the client to report if any ISMS related information (such as ISMS records or information about design and effectiveness of controls) cannot be made available for review by the audit team because it contains confidential or sensitive information. The certification body shall determine whether the ISMS can be adequately audited in the absence of such information. If the certification body concludes that it is not possible to adequately audit the ISMS without reviewing the identified confidential or sensitive information, it shall advise the client that the certification audit cannot take place until appropriate access arrangements are granted.

8.5 Information exchange between a certification body and its clients

The requirements of ISO/IEC 17021-1:2015, 8.5 shall apply.

9 Process requirements

9.1 Pre-certification activities

9.1.1 Application

9.1.1.1 General

The requirements of ISO/IEC 17021-1:2015, shall 9.1.1 apply. In addition, the requirements and guidance in 9.1.1.2 shall apply.

9.1.1.2 Considerations for certification procedures

The certification body's procedures shall not presuppose a particular manner of implementation of an ISMS or a particular format for documentation and records. Certification procedures shall focus on confirming that a client's ISMS meets the requirements specified in ISO/IEC 27001 and the policies and objectives of the client.

NOTE It is possible for an organization to design its own necessary controls or to select them from any source, therefore it is possible that an organization is certified to ISO/IEC 27001 even though none of its necessary controls are those specified in ISO/IEC 27001:2022, Annex A.

9.1.2 Application review

The requirements of ISO/IEC 17021-1:2015, 9.1.2 shall apply.

9.1.3 Audit programme

9.1.3.1 General

The requirements of ISO/IEC 17021-1:2015, 9.1.3 shall apply. In addition, the requirements and guidance in 9.1.3.2, 9.1.3.3, 9.1.3.4, 9.1.3.5 and 9.1.3.6 shall apply.

9.1.3.2 General considerations

The audit programme for ISMS audits shall take the information security controls determined by the client into account.

NOTE 1 The information security controls can be from ISO/IEC 27001:2022, Annex A, and/or other applicable standard(s) and/or self-designed.

NOTE 2 Further guidance on auditing is given in ISO/IEC 27007.

9.1.3.3 Deployment of remote audit

Certification bodies intending to conduct remote audit activities shall define procedures to determine the level of remote audit activities ("remote audits") that can be applied to auditing a client's ISMS. The procedures shall include analysis of the risks related to the use of remote auditing for the client, which shall consider the following factors:

a) available infrastructure of the certification body and the client;

b) sector in which the client operates;

c) type(s) of audit during the certification cycle from initial audit to recertification audit;

d) competence of the persons of the certification body and the client, who are involved in the remote audit;

e) previously demonstrated performance of remote audits for the client;

f) scope of the certification.

The analysis shall be performed prior to performing any remote audit. The analysis and the justification for use of remote audit during the certification cycle shall be documented.

The audit plan and audit report shall include clear indications if remote audit activities have been performed.

Remote audits shall not be used if the risk assessment identifies unacceptable risks to the effectiveness of the audit process.

The risk assessment shall be reviewed during the certification cycle to ensure its continued suitability.

NOTE In case the client uses virtual sites (i.e. location where an organization performs work or provides a service using an online environment allowing persons involved to execute processes irrespective of physical locations), remote audit techniques are a relevant part of the audit plan.

9.1.3.4 General preparations for the initial audit

The certification body shall require that a client makes all necessary arrangements to ensure access to internal audit reports and reports of independent reviews of information security.

9.1.3.5 Review periods

The certification body shall not certify an ISMS unless there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective, and will be maintained covering the scope of certification.

9.1.3.6 Scope of ISMS certification

The audit team shall audit the ISMS of the client covered by the defined scope against all applicable certification requirements. The certification body shall confirm, in the scope of the client’s ISMS, that the client addresses the requirements stated in ISO/IEC 27001:2022, 4.3.

Certification bodies shall ensure that the client’s information security risk assessment and risk treatment properly reflect its activities and extend to the boundaries of its activities, as defined in the scope of the certification. Certification bodies shall confirm that this is reflected in the scope of the client's ISMS and SoA. The certification body shall verify that there is a SoA for the scope of certification.

Certification bodies shall ensure that interfaces with services or activities that are not completely within the scope of the ISMS are addressed within the ISMS subject to certification and are included in the client's information security risk assessment. An example of such a situation is the sharing of facilities (e.g. IT systems, databases and telecommunication systems or the outsourcing of a business function) with other organizations.

9.1.4 Determining audit time

9.1.4.1 General

The requirements of ISO/IEC 17021-1:2015, shall 9.1.4 apply. In addition, the requirements and guidance in 9.1.4.2 shall apply.

9.1.4.2 Audit time

The certification body shall use Annex C to determine audit time.

NOTE Further guidance and examples on audit time calculation are provided in Annex D.

9.1.5 Multi-site sampling

9.1.5.1 General

The requirements of ISO/IEC 17021-1:2015, 9.1.5 shall apply. In addition, the requirements and guidance in 9.1.5.2 shall apply.

9.1.5.2 Multiple sites

9.1.5.2.1 Where a client has a number of sites meeting the criteria from a) to c) below, certification bodies may consider using a sample-based approach to multiple-site certification audit:

a) all sites are operating under the same ISMS, which is centrally administered and audited and subject to central management review;

b) all sites are included within the client's internal ISMS audit programme;

c) all sites are included within the client's ISMS management review programme.

9.1.5.2.2 The certification body wishing to use a sample-based approach shall have procedures to ensure:

a) The initial contract review identifies, to the greatest extent possible, the difference between sites such that an adequate level of sampling is determined.

b) A representative number of sites have been sampled by the certification body, taking into account:

   1) the results of internal audits of the central office (if appropriate) and the sites;

   2) the results of management review;

   3) variations in the size of the sites;

   4) variations in the business purpose of the sites;

   5) complexity of the information systems at the different sites;

   6) variations in working practices;

   7) variations in activities undertaken;

   8) variations of design and operation of controls;

   9) potential interaction with critical information systems or information systems processing sensitive information;

   10) any differing legal requirements;

   11) geographical and cultural aspects;

   12) risk situation of the sites;

   13) information security incidents at the specific sites.

c) A representative sample is selected from all sites within the scope of the client's ISMS; this selection shall be based upon judgmental choice to reflect the factors presented in item b) above, as well as a random element.

d) Every site included in the ISMS which is subject to significant risks is audited by the certification body prior to certification.

e) The audit programme has been designed in light of the above requirements and covers representative samples of the scope of the ISMS certification within the three-year period.

f) In the case of a nonconformity being observed at a single site, the corrective action procedure applies to all sites covered by the certificate.

The audit shall address the client's activities to ensure that a single ISMS applies to all sites and delivers central management at the operational level. The audit shall address all the issues outlined above.

9.1.6 Multiple management systems

9.1.6.1 General

The requirements of ISO/IEC 17021-1:2015, 9.1.6 shall apply. In addition, the requirements and guidance in 9.1.6.2 and 9.1.6.3 shall apply.

9.1.6.2 Integration of ISMS and other management system documentation

The certification body may accept documentation that is combined (e.g. for information security, quality, health and safety and environment) as long as the ISMS can be clearly identified together with the appropriate interfaces to the other management systems.

9.1.6.3 Combining management system audits

The ISMS audit may be combined with audits of other management systems, if it can be demonstrated that the audit satisfies all requirements for certification of the ISMS. All the important elements for an ISMS shall appear clearly and be readily identifiable in the audit reports. The quality of the audit shall not be adversely affected by the combination of the audits.

9.2 Planning audits

9.2.1 Determining audit objectives, scope and criteria

9.2.1.1 General

The requirements of ISO/IEC 17021-1:2015, 9.2.1 shall apply. In addition, the requirements and guidance in 9.2.1.2 and 9.2.1.3 shall apply.

9.2.1.2 Audit objectives

The audit objectives shall include:

a) determining the effectiveness of the management system;

b) ensuring that the client, based on the risk assessment, has identified the necessary controls; and

c) determining that the established information security objectives have been achieved.

9.2.1.3 Audit criteria

The criteria for auditing the ISMS of a client shall include ISO/IEC 27001.

9.2.2 Audit team selection and assignments

9.2.2.1 General

The requirements of ISO/IEC 17021-1:2015, 9.2.2 shall apply.

9.2.3 Audit plan

9.2.3.1 General

The requirements of ISO/IEC 17021-1:2015, 9.2.3 shall apply. In addition, the requirements and guidance in 9.2.3.2 and 9.2.3.3 shall apply.

9.2.3.2 General considerations

The audit plan for ISMS audits shall take the determined information security controls into account.

NOTE It is good practice for a certification body to agree on the timing of the audit with the organization being audited to best demonstrate the full scope of the organization. Considerations can include season, month, day/dates and shifts, as appropriate.

9.2.3.3 Remote audit techniques

The objective of remote auditing techniques should be to enhance audit effectiveness and efficiency, and to support the integrity of the audit process.

The audit plan shall reference tools that are used to assist remote auditing.

9.3 Initial certification

9.3.1 General

The requirements of ISO/IEC 17021-1:2015, 9.3 shall apply. In addition, the requirements and guidance in 9.3.2 shall apply.

9.3.2 Initial certification audit

9.3.2.1 Stage 1

In this stage of the audit, the certification body shall obtain documentation on the design of the ISMS covering the documentation required in ISO/IEC 27001.

As a minimum, the following information shall be provided by the client during stage 1 of the certification audit:

a) general information concerning the ISMS and the activities it covers;

b) a copy of the required ISMS documentation specified in ISO/IEC 27001 and, where required, other associated documentation.

The certification body shall obtain sufficient understanding of the design of the ISMS in the context of the client's organization, risk assessment and treatment (including the controls determined), information security policy and objectives and, in particular, of the client's preparedness for the audit. This shall be used for planning the stage 2 audit.

The results of stage 1 shall be documented in a written report. The certification body shall review the stage 1 audit report before deciding on proceeding with stage 2. The certification body shall confirm the stage 2 audit team members have the necessary competence. This may be done by the auditor leading the team that conducted the stage 1 audit if deemed competent and appropriate.

NOTE Having a person from the certification body who is not involved in the audit reviewing the report, and who decides to proceed and confirms the competence of the audit team members for stage 2, offers a degree of mitigation for the risks involved. However, other risk mitigation measures can already be in place to achieve the same goal.

The certification body shall make the client aware of the further types of information and records that may be required for detailed examination during stage 2.

9.3.2.2 Stage 2

Based on the findings documented in the stage 1 audit report, the certification body shall develop an audit plan for the conduct of stage 2. In addition to evaluating the effective implementation of the ISMS, the objective of stage 2 is to confirm that the client adheres to its own policies, objectives and procedures.

To do this, the audit shall focus on the client's:

a) top management leadership and commitment to the information security objectives;

b) assessment of information security related risks; the audit shall also ensure that the assessments produce consistent, valid and comparable results, if repeated;

c) determination of controls based on the information security risk assessment and risk treatment processes;

d) information security performance and the effectiveness of the ISMS, evaluating these against the information security objectives;

e) correspondence between the determined controls, the Statement of Applicability, the results of the information security risk assessment, the risk treatment process and the information security policy and objectives;

f) implementation of controls (see Annex E for examples on auditing controls) taking into account the external and internal context and related risks, and the organization's monitoring, measurement and analysis of information security processes and controls, to determine whether controls declared as being implemented are actually implemented and effective as a whole;

g) programmes, processes, procedures, records, internal audits and reviews of the ISMS effectiveness to ensure that these are traceable to top management decisions and the information security policy and objectives.

9.4 Conducting audits

9.4.1 General

The requirements of ISO/IEC 17021-1:2015, 9.4 shall apply. In addition, the requirements and guidance in 9.4.2 and 9.4.3 shall apply.

9.4.2 Specific elements of the ISMS audit

The certification body audit team shall:

a) require the client to demonstrate that the assessment of information security related risks is relevant and adequate for the ISMS operation within the ISMS scope;

b) establish whether the client’s procedures for the identification, examination and evaluation of information security related risks and the results of their implementation are consistent with the client’s policy, objectives and targets.

The certification body shall also establish whether the procedures employed in risk assessment are sound and properly implemented.

9.4.3 Audit report

9.4.3.1 The audit report shall provide the following information or a reference to it:

a) an account of the audit of the client's information security risk analysis;

b) any information security control sets used by the organization for comparison purposes as required by ISO/IEC 27001:2022, 6.1.3 c).

9.4.3.2 The audit report shall be sufficiently detailed to facilitate and support the certification decision. It shall contain:

a) the significant audit trails followed and audit methodologies utilized (see 9.1.1.2);

b) a reference to the version of the Statement of Applicability and, where applicable, any useful comparison with the results of previous certification audits of the client.

Completed questionnaires, checklists, observations, logs, or auditor notes may form an integral part of the audit report. If these methods are used, these documents shall be submitted to the certification body as evidence to support the certification decision. Information about the samples evaluated during the audit shall be included in the audit report, or in other certification documentation.

Where remote audit methods have been used, the report shall indicate the extent to which they have been used in carrying out the audit and their effectiveness in achieving the audit objectives.

Where the activities of the organization are not undertaken at a defined physical location and therefore all activities of the organization are conducted remotely, the audit report shall state that all activities of the organization are conducted remotely.

The report shall consider the adequacy of the internal organization and procedures adopted by the client to give confidence in the ISMS.

The report shall include a summary of the most important observations, positive as well as negative, regarding the implementation and effectiveness of the ISMS requirements and information security controls.

9.5 Certification decision

9.5.1 General

The requirements of ISO/IEC 17021-1:2015, 9.5 shall apply. In addition, the requirements and guidance in 9.5.2 apply.

9.5.2 Certification decision

The certification decision shall be based on the certification recommendation of the audit team as provided in their certification audit report.

Certification shall not be granted to the client until there is sufficient evidence to demonstrate that arrangements for management reviews and internal ISMS audits have been implemented, are effective and will be maintained.

9.6 Maintaining certification

9.6.1 General

The requirements of ISO/IEC 17021-1:2015, 9.6.1 shall apply.

9.6.2 Surveillance activities

9.6.2.1 The requirements of ISO/IEC 17021-1:2015, 9.6.2 shall apply. In addition, the requirements and guidance in 9.6.2.2, 9.6.2.3 and 9.6.2.4 shall apply.

9.6.2.2 Surveillance audit procedures shall be a subset of those for the certification audit of the client's ISMS as described in this document.

The purpose of surveillance is to verify that the approved ISMS continues to be implemented, to consider the implications of changes to the ISMS initiated as a result of changes in the client’s operational practices and to confirm continued compliance with certification requirements. Surveillance audit programmes shall cover at least:

a) the ISMS maintenance elements such as information security risk assessment and control maintenance, internal ISMS audit, management review and corrective action;

b) communications from external parties as required by ISO/IEC 27001 and other documents required for certification.

9.6.2.3 As a minimum, every surveillance audit by the certification body shall review the following:

a) the effectiveness of the ISMS with regard to achieving the objectives of the client's information security policy;

b) the functioning of procedures for the periodic evaluation and review of compliance with relevant information security legislation and regulations;

c) changes to the controls determined, and resulting changes to the SoA;

d) implementation and effectiveness of controls indicated in the audit programme.

9.6.2.4 The certification body shall be able to adapt its programme of surveillance activities to reflect the information security issues related to risks and impacts on the client and justify this programme.

Surveillance audits may be combined with audits of other management systems. Audit reports shall clearly indicate the aspects relevant to each management system.

During surveillance audits, certification bodies shall check the records of appeals and complaints brought before the certification body. Where any nonconformity or failure to meet the requirements of certification is revealed, certification bodies shall check that the client has investigated its own ISMS and procedures, and has taken appropriate corrective action.

A surveillance report shall contain, in particular, information on clearing of nonconformities revealed previously, the version of the SoA and important changes from the previous audit. As a minimum, the reports arising from surveillance shall build up to cover in totality the requirements of 9.6.2.2 and 9.6.2.3.

9.6.3 Re-certification

9.6.3.1 General

The requirements of ISO/IEC 17021-1:2015, 9.6.3 shall apply. In addition, the requirements in 9.6.3.2 shall apply.

9.6.3.2 Re-certification audits

Re-certification audit procedures shall be a subset of those for the initial certification audit of the client's ISMS as described in this document.

The time allowed to implement corrective action shall be consistent with the severity of the nonconformity and the associated information security risk.

9.6.4 Special audits

The requirements of ISO/IEC 17021-1:2015, 9.6.4 shall apply.

9.6.5 Suspending, withdrawing or reducing the scope of certification

The requirements of ISO/IEC 17021-1:2015, 9.6.5 shall apply.

9.7 Appeals

The requirements of ISO/IEC 17021-1:2015, 9.7 shall apply.

9.8 Complaints

9.8.1 General

The requirements of ISO/IEC 17021-1:2015, 9.8 shall apply.

9.8.2 Complaints

Complaints represent a potential incident and an indication of possible nonconformity.

9.9 Client records

The requirements of ISO/IEC 17021-1:2015, 9.9 shall apply.

10 Management system requirements for certification bodies

10.1 Options

10.1.1 General

The requirements of ISO/IEC 17021-1:2015, 10.1 shall apply. In addition, the requirements and guidance in 10.1.2 shall apply.

10.1.2 ISMS implementation

It is recommended that certification bodies implement an ISMS in accordance with ISO/IEC 27001.

10.2 Option A: General management system requirements

The requirements of ISO/IEC 17021-1:2015, 10.2 shall apply.

10.3 Option B: Management system requirements in accordance with ISO 9001

The requirements of ISO/IEC 17021-1:2015, 10.3 shall apply.

Annex A
(normative)

Knowledge and skills for ISMS auditing and certification

A.1 Overview

Table A.1 specifies the knowledge and skills that a certification body shall define for specific certification functions, in addition to the requirements in ISO/IEC 17021-1. "X" indicates that the certification body shall define the criteria and depth of knowledge and skills. The knowledge and skill requirements specified in Table A.1 are explained in more detail in Clause 7 and are cross-referenced in parentheses in Table A.1.

Table A.1 — Table of knowledge and skills for ISMS auditing and certification

	Certification function		
Knowledge and skills	**Conducting the application review to determine audit team competence required, to select the audit team members, and to determine the audit time**	**Reviewing audit reports and making certification decisions**	**Auditing and leading the audit team**
Information security management terminology, principles, practices and techniques		X (see 7.1.3.3.2)	X (see 7.1.3.1.2)
Information security management system standards/ normative documents			X (see 7.1.3.1.3)
Business management practices			X (see 7.1.3.1.4)
Client business sector	X (see 7.1.3.2.1)	X (see 7.1.3.3.3)	X (see 7.1.3.1.5)
Client products, processes and organization	X (see 7.1.3.2.2)	X (see 7.1.3.3.4)	X (see 7.1.3.1.6)

NOTE Further competence considerations are contained in Annex B.

Annex B
(informative)

Further competence considerations

B.1 General competence considerations

There are several ways by which auditors can demonstrate their knowledge and experience. Knowledge and experience can be evaluated, for example, by using recognized qualifications. Registration records under a personnel certification scheme can also be used to evaluate the required knowledge and experience. The required competence level for the audit team should be established, reflecting the organization's industry/technological field and complexity of the ISMS.

B.2 Specific knowledge and experience considerations

B.2.1 Typical knowledge related to ISMS

In addition to the requirements in 7.1.3, the following should be considered. Auditors should have knowledge and understanding of the following auditing and ISMS subjects:

- audit programming and planning;
- audit type and methodologies;
- audit risk;
- information security processes analysis;
- continual improvement;
- internal auditing of information security.

Auditors should have knowledge and understanding of regulatory requirements on the following:

- intellectual property;
- content, protection and retention of organizational records;
- data protection and privacy;
- regulation of cryptographic controls;
- electronic commerce;
- electronic and digital signatures;
- workplace surveillance;
- telecommunications interception and monitoring of data (e.g. email);
- computer abuse;
- electronic evidence collection;
- penetration testing;
- international and national sector-specific requirements (e.g. banking).

It is possible that for a particular sector, knowledge and understanding is established in a specific standard (e.g. ISO/IEC 27006-2).

Annex C
(normative)

Audit time

C.1 General

This annex contains further requirements related to ISO/IEC 17021-1:2015, 9.1.4. It provides minimum requirements and guidance for a certification body on the development of its own procedures to determine the amount of time required for the certification of ISMS scopes of differing sizes and complexity over a broad spectrum of activities.

Certification bodies shall allow auditors sufficient time to undertake all activities relating to an initial audit, surveillance audit or re-certification audit. The calculation of overall audit time shall include sufficient time for audit reporting.

Certification bodies shall identify the amount of audit time to be spent on initial certification, surveillance and re-certification for each client and certified ISMS. Using this annex during the audit-planning phase leads to a consistent approach to determine the appropriate audit time. Additionally, the audit time may be adjusted based on what is found during the course of the audit, especially during stage 1 (e.g. different assessment of the complexity of the ISMS scope, or additional sites in the scope).

This annex presents:

— concepts that are used for audit time calculation (C.2);

— requirements for the procedures to determine audit time for the different stages of the initial audit (C.3);

— requirements for audit time for surveillance (C.4) and re-certification audit (C.5);

— requirements related to multi-site audits (C.6);

— requirements for audit time for scope extensions (C.7).

Examples for audit time calculation to illustrate the application of this annex can be found in Annex D.

A basic assumption of the approach in this annex is that a calculation scheme to determine audit time should:

a) consider only attributes that can be valued objectively;

b) be simple enough for certification bodies to apply and achieve valid comparable and reproducible results;

c) be sophisticated enough to ensure that variations in attribute values result in comparable changes in the resulting audit time.

The determination of the audit time is based on the numbers provided in Table C.1 and shall consider contributing factors for modification.

The approach to determine audit time defined by the certification body shall be regularly reviewed to verify if it is sufficient for the complexity of the ISMS.

C.2 Concepts

C.2.1 Number of persons doing work under the organization’s control

The total number of persons doing work under the organization’s control for all shifts within the scope of certification is the starting point to determine the audit time.

NOTE Persons doing work under the organization’s control includes all personnel (regardless of whether they are members of the organization or not) within the scope of the certification who are required to work according to the requirements of the ISMS.

Part-time persons doing work under the organization's control contribute to the number of persons doing work under the organization's control proportionally to the number of hours worked as compared with a full-time person doing work under the organization's control. This determination shall depend upon the number of hours worked as compared with a full-time employee.

When a high percentage of persons doing work under the organization’s control within the scope of certification perform certain identical activities, a reduction of the number of persons prior to the use of Table C.1 is permitted for the calculation of audit time. Certification bodies shall use the factors given in C.3.4 and consider the influence of the activities on information security risk to determine how a reduction of the number of persons is applied within the scope of certification. Coherent and consistent procedure(s) that are repeatable and can be applied on a company-to-company basis shall be documented.

C.2.2 Auditor day

Audit time as referenced in Table C.1 is stated in terms of auditor days spent on the audit. This annex bases its calculation on an eight-hour working day (abbreviated as “d”).

C.2.3 Temporary site

A temporary site that falls within the scope of certification is a location other than the sites identified in the certification documents where activities, within the scope of certification, are implemented for a defined period of time. These sites can range from major project management sites to minor service/installation sites. The need to visit such sites and the extent of sampling should be based on an evaluation of the risks of activities performed at this temporary site in meeting the information security objectives. The sample of such sites selected should represent the range of the organization’s competency needs and service variations in light of the sizes and types of activities and the various stages of projects in progress. For general sampling, see 9.1.5.2.

C.3 Procedure to determine audit time for initial audit

C.3.1 General

The certification body shall have and follow a documented procedure for the calculation of audit time.

C.3.2 Remote methods for conducting audit

If remote auditing methods such as interactive web-based collaboration, web meetings, teleconferences and/or electronic verification of the organization’s processes are utilized to interface with the organization, these activities should be identified in the audit plan (see 9.2.3) and may be considered as partially contributing to the total “on-site audit time”.

NOTE On-site audit time refers to the on-site audit time allocated for individual sites. Electronic audits of remote sites are considered to be remote audits, even if the electronic audits are physically carried out on the organization’s premises.

C.3.3 Audit time calculation

The audit time chart provided in Table C.1 sets out the starting point for an average number of initial audit days [within this annex and Annex D this number encompasses the days for an initial audit (Stage 1 and Stage 2)], which experience has shown to be appropriate for an ISMS scope with a given number of persons doing work under the organization's control. Experience has also demonstrated that for ISMS scopes of a similar size, some require more time than others.

The audit time chart below provides the framework that shall be used for audit planning. The starting point is based on the total number of persons doing work under the organization's control for all shifts. The number of auditor days is adjusted based on the significant factors applying to the ISMS scope to be audited, attributing an additive or subtractive weighting for each factor to modify the base figure. The audit time chart in Table C.1 shall be used, taking account of the contributing factors and restrictions of permitted deviation (see C.3.5 and C.3.6). The terms used in Table C.1 are explained in C.2. Annex D provides examples of how the calculation method of this annex can be applied.

C.3.4 Determination of initial number of persons

Certification bodies shall request information from the client related to the high number of persons performing certain identical activities, to include:

- the number of persons engaged in the activity;
- the type of activity or process.

Examples of factors that can reduce the number of persons used as a basis for calculation who are performing certain identical activities, include:

- persons with read-only access to information to perform their duties;
- persons with no access to the organization’s information processing facilities in scope of the ISMS;
- persons who have specific demonstrable restricted access to the company’s information processing facilities in scope of the ISMS;
- persons who perform activities where strict limitations are implemented to restrict disclosure of information, e.g. measures prohibiting personal belongings and devices into the work area.

A reduction in the number of persons performing identical activities shall be made based on the risk of the activities associated with the tasks. The square root of the head count of people performing each identical activity may be used to determine the effective number of people, which is used for audit duration calculations, rounded up to the next full number. This number shall be the maximum reduction of the head count allowed.

The nature of the tasks, the legislative requirements, and the importance of information to which persons have access can limit the reduction.

The number of persons determined after this procedure is the starting point in Table C.1.

NOTE The table is structured identically to IAF MD5.[9]

Table C.1 — Audit time chart

Number of persons doing work under the organization's control	Quality management system audit time for initial audit (auditor days, d)	Environmental management system audit time for initial audit (auditor days, d)	ISMS audit time for initial audit (auditor days, d)	Additive and subtractive factors	Total audit time
1–10	1,5–2	2,5–3	5	See C.3.5	
11–15	2,5	3,5	6	See C.3.5	
16–25	3	4,5	7	See C.3.5	
26–45	4	5,5	8,5	See C.3.5	
46–65	5	6	10	See C.3.5	
66–85	6	7	11	See C.3.5	
86–125	7	8	12	See C.3.5	
126–175	8	9	13	See C.3.5	
176–275	9	10	14	See C.3.5	
276–425	10	11	15	See C.3.5	
426–625	11	12	16,5	See C.3.5	
626–875	12	13	17,5	See C.3.5	
876–1 175	13	15	18,5	See C.3.5	
1 176–1 550	14	16	19,5	See C.3.5	
1 551–2 025	15	17	21	See C.3.5	
2 026–2 675	16	18	22	See C.3.5	
2 676–3 450	17	19	23	See C.3.5	
3 451–4 350	18	20	24	See C.3.5	
4 351–5 450	19	21	25	See C.3.5	
5 451–6 800	20	23	26	See C.3.5	
6 801–8 500	21	25	27	See C.3.5	
8 501–10 700	22	27	28	See C.3.5	
> 10 700	Follow progression above	Follow progression above	Follow progression above	See C.3.5	

C.3.5 Factors for adjustment of audit time

Table C.1 shall not be used in isolation. The time allocated shall also consider the following factors which relate to the complexity of the ISMS and therefore to the effort needed to audit the ISMS:

a) complexity of the ISMS (e.g. criticality of information, risk associated with the ISMS, etc.);

b) the type(s) of business performed within scope of the ISMS;

c) previously demonstrated performance of the ISMS;

d) extent and diversity of technology utilized in the implementation of the various components of the ISMS (e.g. number of different IT platforms, number of segregated networks);

e) extent of outsourcing and third-party arrangements used within the scope of the ISMS;

f) extent of information system development;

g) number of sites and number of Disaster Recovery (DR) sites;

h) after stage one the certification body will consider the number and complexity of controls;

i) for surveillance or re-certification audit: The amount and extent of change relevant to the ISMS in accordance with ISO/IEC 17021-1:2015, 8.5.3.

Annex D provides examples of how these different factors can be taken into account when calculating audit time.

Examples of factors requiring addition of audit time are:

- complicated process logistics involving more than one building or location in the scope of the ISMS;
- staff speaking more than one language (requiring interpreter(s) or preventing individual auditors from working independently) or documentation provided in more than one language;
- activities that require visiting temporary sites to confirm the activities of the permanent sites(s) whose management system is subject to certification (see paragraph below next list);
- high number of standards and regulations that apply to the ISMS.

Examples of factors permitting subtraction of audit time are:

- no or low-risk processes;
- processes involving a single general activity (e.g. service only);
- prior knowledge of the organization (e.g. if the organization has already been certified to another standard by the same certification body);
- high client preparedness for certification (e.g. already certified or recognized by another third-party scheme);
- high maturity of the management system in place.

In situations where the client or certified organization provides their product(s) or service at temporary sites, it is important that evaluations of such sites are incorporated into the certification audit and surveillance programmes.

Adjustments can be made for the above factors. Factors requiring the addition or subtraction of audit time may off-set each other. In all cases where adjustments are made to the time provided in the audit Table C.1, sufficient evidence and records shall be maintained to justify the variation.

C.3.6 Limitation of deviation of audit time

In order to ensure effective audits are performed and to ensure reliable and comparable results, the audit time provided in the audit time chart shall not be reduced by more than 30 %.

Appropriate reasons for deviation shall be established and documented.

C.3.7 On-site audit time

It is expected that the time calculated for planning and report writing combined should not typically reduce the total on-site "audit time" (physical/remote) to less than 70 % of the time calculated in accordance with C.3.3, C.3.4 and C.3.5. Where additional time is required for planning and/or report writing, this shall not be a justification for reducing on-site audit time. Auditor travel time is not included in this calculation and is additional to the audit time referenced in the chart.

NOTE 1 70 % is a factor based on experience of ISMS audits.

NOTE 2 The term "(physical/remote)" means that "on site" audits (for physical locations or electronic sites of the client) can be conducted physically or remotely (see 9.2.3 and C.3.2). For "on-site" audits, see also ISO/IEC 17021-1:2015, 9.4.1.

C.4 Audit time for surveillance audits

For the initial certification audit cycle, surveillance time for a given organization should be proportional to the time spent at initial audit, with the total amount of time spent annually on surveillance being about 1/3 of the time spent on the initial audit. The planned surveillance time should be reviewed occasionally, to account for changes that can affect audit time. The time spent on a surveillance audit shall be increased to allow for the audit of changes in the ISMS (such as the audit of new or changed information security controls, processes and services).

C.5 Audit time for re-certification audit

The total amount of time spent performing the re-certification audit shall depend upon the results of any prior audit as defined in 9.4.3 and ISO/IEC 17021-1:2015, 9.6.3. The audit time for a re-certification audit should be proportional to, but at least two thirds of, the audit time required for an initial certification audit of the same organization at the time of the re-certification audit.

C.6 Audit time of multi-site

Generally, the total audit time for on-site audit shall be calculated by considering the total number of persons doing work under the organization's control irrespective of their location.

Alternatively, for justified reasons which shall be documented, it is permitted to sum the audit times which are individually calculated for each site, as long as this total audit time is larger than that defined in accordance with the first paragraph of this clause. Reductions may be applied to consider the parts of the audit that are not relevant to the central office or the local sites (if applicable). Reasons for the justification of such reductions shall be recorded by the certification body.

The number of total on-site auditor days – as calculated for the scope following the procedure stated in C.3.3 and C.3.4 and this clause – shall be allocated across the different sites based on the relevance of the site for the management system, the activities conducted at the site and the risks identified. The justification for the allocation shall be recorded by the certification body.

Any reductions shall be applied before comparing the audit time with the overall audit time.

C.7 Audit time for scope extensions

The audit time required to extend the scope of an ISMS shall be calculated considering factors such as:

a) the type of extension:

b) the activity/ activities of the current certification;

c) the number of locations where the activity/activities take(s) place;

d) the related information security risks related to the activity/activities;

e) the number of controls relevant to the extension;

f) the number of persons doing work under the organization's control of the new scope; and

g) the time required to review the integration of the extended scope into the ISMS.

Certification bodies shall have procedures that provide a consistent approach to extension of the scope.

For the initial audit of the new scope, the time shall be calculated based on the number of persons and sites being added to the already existing scope using C.3.3, C.3.4 and C.3.5.

Audit time shall be added to the calculated duration to review the client's ISMS. This additional time shall be at least:

1) 0,5 d (auditor days) if the extension to scope audit is conducted in conjunction with a surveillance audit or a recertification audit.

2) 1,0 d (auditor days) when the extension to scope audit is conducted as a separate audit.

Annex D
(informative)

Methods for audit time calculations

D.1 General

This annex provides further guidance on developing a formula to calculate audit time. D.2 gives an example of a classification of factors that can be used as the basis for calculating audit time and D.3 provides an example of a calculation of audit time.

NOTE The concepts in this annex start after any reductions of persons performing certain identical activities have been applied, as described in C.3.4.

D.2 Classification of factors for calculating audit time

Table D.1 gives examples for the classification of the main factors for the calculation of audit time, as listed in C.3.5, a) to i). This classification can be used by certification bodies to derive an audit time calculation scheme in line with 9.1.4.2.

Table D.1 — Classification of factors for calculating audit time

	Impact on effort		
	Reduced effort	**Normal effort**	**Increased effort**
Factors (see C.3.5)			
a) complexity of the ISMS: — information security requirements [confidentiality, integrity and availability, (CIA)] — number of critical assets — number of processes and services	— Only little sensitive or confidential information, low availability requirements — Few critical assets (in terms of CIA) — Only one key business process with few interfaces and few business units involved	— Higher availability requirements or some sensitive/confidential information — Some critical assets — 2–3 simple business processes with few interfaces and few business units involved	— Higher amount of sensitive or confidential information (e.g. health, personally identifiable information, insurance, banking) or high availability requirements — Many critical assets — More than 2 complex processes with many interfaces and business units involved
b) the type(s) of business performed within the scope of the ISMS	— Low risk business without regulatory requirements	— High regulatory requirements	— High risk business with (only) limited regulatory requirements
c) previously demonstrated performance of the ISMS	— Recently certified — Not certified but ISMS fully implemented over several audit and improvement cycles, including documented internal audits, management reviews and effective continual improvement system	— Recent surveillance audit — Not certified but partially implemented ISMS: Some management system tools are available and implemented; some continual improvement processes are in place but partially documented	— No certification and no recent audits — ISMS is new and not fully established (e.g. lack of management system specific control mechanisms, immature continual improvement processes, ad hoc process execution)

Table D.1 *(continued)*

		Impact on effort		
		Reduced effort	**Normal effort**	**Increased effort**
d)	extent and diversity of technology utilized in the implementation of the various components of the ISMS (e.g. number of different IT platforms, number of segregated networks)	— Highly standardized environment with low diversity (few IT-platforms, servers, operating systems, databases, networks, etc.)	— Standardized but diverse IT platforms, servers, operating systems, databases, networks	— High diversity or complexity of IT (e.g. many different segments of networks, types of servers or databases, number of key applications)
e)	extent of outsourcing and third-party arrangements used within the scope of the ISMS	— No outsourcing and little dependency on suppliers, or — Well-defined, managed and monitored outsourcing arrangements — Outsourcer has a certified ISMS — Relevant independent assurance reports are available	— Several partly managed outsourcing arrangements	— High dependency on outsourcing or suppliers with large impact on important business activities, or — Unknown amount or extent of outsourcing, or — Several unmanaged outsourcing arrangements
f)	extent of information system development	— No in-house system development — Use of standardized software platforms	— Use of standardized software platforms with complex configuration/ parameterization — (Highly) customized software — Some development activities (in-house or outsourced)	— Extensive internal software development activities with several ongoing projects for important business purpose
g)	number of sites and number of disaster recovery (DR) sites	— Low availability requirements and no or one DR site	— Medium or high availability requirements and no or one DR site	— High availability requirements e.g. 24/7 services — Several DR sites — Several data centres
h)	the number and complexity of controls	— Smaller than usual number of controls with some common control areas not included – e.g. no systems development controls or no physical controls	— Typical number and complexity of controls	— More than usual number of detailed and complex controls, e.g. many controls related to networking protocols or cryptography
i)	for surveillance or re-certification audit: the amount and extent of change relevant to the ISMS in accordance with ISO/IEC 17021-1:2015, 8.5.3	— No changes since last re-certification audit	— Minor changes in scope or SoA of ISMS, e.g. some policies, documents — Minor changes in the factors above	— Major changes in scope or SoA of ISMS, e.g. new processes, new business units, areas, risk assessment management methodology, policies, documentation, risk treatment — Major changes in the factors above

D.3 Example for audit time calculation

The following example illustrates how a certification body may use the factors provided in C.3 to calculate audit time. The calculation of audit time in the example below works in the following way:

Step 1: Determination of factors related to business and organization (other than IT): Identify the suitable grade for each of the categories given in Table D.2 and sum up the results.

Step 2: Determination of factors related to IT environment: Identify the suitable grade for each of the categories given in Table D.3 and sum up the results.

Step 3: Based on the results of step 1 and 2 above, identify the impact of factors on audit time by selecting the appropriate entry in Table D.4.

Step 4: Final calculation: The number of days determined by applying the audit time chart (Table C.1) is multiplied by the factor resulting from Step 3. Where multi-site sampling is utilized, the audit days calculated are increased based on the efforts needed to execute the multi-site sampling plan.

This result is the final number of audit days.

Table D.2 — Factors related to business and organization (other than IT)

Category	Grade
Type(s) of business and regulatory requirements	1. Organization works in non-critical business sectors and non-regulated sectors[a] 2. Organization has customers in critical business sectors [a] 3. Organization works in critical business sectors [a]
Process and tasks	1. Standard processes with standard tasks; few products or services 2. Standard but non-repetitive processes, with high number of products or services 3. Complex processes, high number of products and services, many business units included in the scope of certification (ISMS covers highly complex processes or relatively high number or unique activities)
Level of establishment of the management system	1. ISMS is already well established and/or other management systems are in place 2. Some elements of other management systems are implemented, others not 3. No other management system implemented at all, the ISMS is new and not established

[a] Critical business sectors are sectors that can affect critical public services that cause risk to health, security, economy, reputation and government ability to function, and can have significant negative impact on countries.

Table D.3 — Factors related to IT environment

Category	Grade
IT infrastructure complexity	1. Few or highly standardized IT platforms, servers, operating systems, databases, networks, etc. 2. Several different IT platforms, servers, operating systems, databases, networks 3. Many different IT platforms, servers, operating systems, databases, networks
Dependency on outsourcing and suppliers, including cloud services	1. Little or no dependency on outsourcing or suppliers 2. Some dependency on outsourcing or suppliers, related to some but not all important business activities 3. High dependency on outsourcing or suppliers, large impact on important business activities
Information system development	1. None or a very limited in-house system/application development 2. Some in-house or outsourced system/application development for some important business purposes 3. Extensive in-house or outsourced system/application development for important business purposes

Table D.4 — Impact of factors on audit time

		IT complexity		
		Low (from 3 to 4)	**Medium (from 5 to 6)**	**High (from 7 to 9)**
Business complexity	**High (from 7 to 9)**	+5 % to +20 %	+10 % to +50 %	+20 % to +100 %
	Medium (from 5 to 6)	−5 % to −10 %	0 %	+10 % to +50 %
	Low (from 3 to 4)	−10 % to −30 %	−5 % to −10 %	+5 % to +20 %

EXAMPLE 1 The organization to be audited has 700 employees, thus according to Table C.1, 17,5 days are required for the initial audit. The organization does not work in a critical business sector, has highly standardized and repetitive tasks and has recently established the ISMS. According to Table D.2, this would yield a factor related to business and organization of 1+1+3 = 5. The organization has very few IT-platforms and databases but uses outsourcing extensively. Software development is not undertaken within, or outsourced by, the organization. According to Table D.3, this would yield a factor related to the IT environment of 1+3+1 = 5. Using Table D.4, this would yield no adjustment for the audit time.

EXAMPLE 2 Using the same organization as in example 1, except that several management systems are already in place and the ISMS is already well established, would change the calculation according to Table D.2 to 1+1+1 = 3. According to Table D.4, this would yield a reduction of 5 % to 10 % of the audit time, i.e. the audit time would be reduced by 1 day to 1,5 days, yielding a total of 16 days to 16,5 days.

Annex E
(informative)

Guidance for review of implemented ISO/IEC 27001:2022, Annex A controls

E.1 Purpose

According to the requirement in 9.3.2.2 f), the implementation of controls that were determined as necessary by the client for the ISMS (as per the Statement of Applicability) shall be reviewed during stage 2 of the initial audit and during surveillance or re-certification activities. The reviews are intended to determine whether the controls are implemented and effective, and whether they meet their stated information security objectives.

It is not usually until after an auditor visits an organization that the certification body knows what the organization's necessary controls are, or even if they are described using the same control text as in ISO/IEC 27001:2022, Annex A. Nor does the certification body know the relationship between information security controls, or the relationship between information security controls and the organization's processes. Thus, the initial audit can be constrained to audit individual controls, whereas subsequent audits can adopt the more effective approach of auditing controls in the context of the organization's processes and risk treatment plans in which they are deployed.

Nevertheless, certification bodies do know that organizations are required to compare their necessary controls with those in ISO/IEC 27001:2022, Annex A and therefore a relationship exists between the organization's necessary controls and those in ISO/IEC 27001:2022, Annex A. The guidance given in Table E.1 is intended to support the certification body in developing audit plans to accommodate the necessary controls determined by the client given their relationship with the controls in ISO/IEC 27001:2022, Annex A.

E.2 How to use Table E.1

E.2.1 General

Table E.1 provides example guidance on reviewing necessary controls. It uses the controls listed in ISO/IEC 27001:2022, Annex A, but auditors should use the relationship between these controls and the organization's necessary controls for interpreting the guidance given in Table E.1 for the gathering audit evidence to demonstrate the controls effectiveness.

NOTE Table E.1 is not intended to provide guidance for reviewing controls unrelated to those in ISO/IEC 27001:2022, Annex A.

Most controls contain organizational aspects which can be evidenced, e.g. by reviewing the client's documentation on controls, processes or procedures, by interviews or by observation.

Many controls are based on rules made by the client organization. Such rules can be in the form of topic-specific policies, requirements in processes or procedures, or other types of rules that are communicated to personnel. Table E.1 uses the generic term "rules" to denote such requirements or expectations set by the management of the client organization.

Many controls can be tested by sampling, i.e. reviewing a sample of the outcomes of the control activity.

E.2.2 Column "system testing"

Many controls in ISO/IEC 27001:2022, Annex A are implemented as technological controls, e.g. through specific system settings, configurations or functionality of technology. Evidence of the performance of technological controls can often be gathered through system testing or through use of specialized audit or reporting tools. System testing means direct review of information systems: the auditor can review system settings and configurations or evaluate results of testing tools. If the client has tools in use that are known to the auditor, these can also be used to support the audit, or the auditor can review the results of an evaluation performed by the client.

The column "system testing" in Table E.1 provides guidance for the review of technological controls:

- "blank" means that system testing is usually not applicable or not necessary in an ISMS audit;
- "possible" means that system testing is usually possible for the evaluation of control implementation, but may not be necessary in an ISMS audit;
- "recommended" means that system testing is usually necessary in an ISMS audit.

E.2.3 Column "visual inspection"

Other controls in ISO/IEC 27001:2022, Annex A can be reviewed through a "visual inspection" on site to evaluate their implementation and effectiveness. Relying on reviewing the respective documentation on paper or interviews is insufficient and so the auditor should consider verifying the control at the location where it is implemented.

NOTE Visual inspection on site can also be achieved using remote inspection techniques, e.g. having a person on site with a real-time video feed to the auditor.

The column "visual inspection" in Table E.1 provides guidance for reviewing physical evidence of controls:

- "blank" means that visual inspection is usually not applicable or not necessary in an ISMS audit;
- "possible" means that visual inspection is usually possible for the evaluation of control implementation, but may not be necessary in an ISMS audit;
- "recommended" means that visual inspection is usually necessary in an ISMS audit.

E.2.4 Possible evidence of design and implementation of controls

The column "possible evidence of design and implementation of controls" provides guidance on evidence that can assist an auditor to assess conformity with ISO/IEC 27001:2022, 8.3 (the requirement to implement the risk treatment plan, and thereby the necessary controls). The various bullet points in this column are not requirements and do not constitute an exhaustive list. As they are derived from the control text in ISO/IEC 27001:2022, Annex A, they are not necessarily appropriate for an organization's corresponding necessary control(s). If this is the case, other forms of evidence should be used. The organization's Statement of Applicability and related ISMS documentation should be used as the specification for the organization's necessary controls. The organization's Statement of Applicability contains the necessary controls, the justification for their inclusion, whether they are implemented or not, and the justification for any controls excluded from ISO/IEC 27001:2022, Annex A.

Table E.1 — Evaluation of controls

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
5 Organizational controls			
5.1 Policies for information security			— Information security policy — Topic-specific policies for information security, as considered necessary by the organization — Dissemination of policies to relevant personnel and interested parties

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
5.2 Information security roles and responsibilities			— Allocated roles and responsibilities for implementation, operation and management of information security
5.3 Segregation of duties			— Identified conflicting duties or areas of responsibility, and corresponding rules for segregation
5.4 Management responsibilities			— Management statements and support for information security objectives, policies, procedures, etc. — Mentioning of personal responsibility for information security of personnel
5.5 Contact with authorities			— Defined contact points with relevant authorities — Rules for reporting incidents — Content of information flow from and to relevant authorities
5.6 Contact with special interest groups			— Membership and defined contact points with special interest groups, or other forums and associations [e.g. Computer Emergency Response Teams (CERTs), cybersecurity agencies] — Rules on what can be discussed within such organizations — Content of information flow from and to such organizations
5.7 Threat intelligence			— Approach to collecting relevant threat intelligence — Analysis of threat intelligence in relation to the organization and its dissemination to appropriate parties
5.8 Information security in project management			— Established information security in project management throughout the project life cycle, e.g. in requirements definition, testing — For a sample of projects, identified information security risks and corresponding risk treatment
5.9 Inventory of information and other associated assets	possible		— Inventories of information and other associated assets maintained by the ISMS — Maintained ownership of assets in asset inventories — Rules for owner duties for assets, e.g. classification
5.10 Acceptable use of information and other associated assets			— Documented rules for the acceptable use of information and other associated assets — Procedures for handling information and other associated assets
5.11 Return of assets			— Rules for the return of organization's assets, e.g. checklists for change or termination of employment, contract, or agreement — Sample of documented return records
5.12 Classification of information			— Rules and scheme for the classification of information, e.g. in a topic-specific policy — Sample of information from various sources that should be classified

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
5.13 Labelling of information		possible	— Rules for the labelling of information and other associated assets — Procedures for labelling specific types of information and other associated assets
5.14 Information transfer	possible		— Rules for information transfer, e.g. in a topic-specific policy — Definition of use cases of information transfer identified in the ISMS and corresponding rules, procedures or agreements, covering e.g. physical, electronic or verbal transfer — Samples of implemented information transfer procedures or agreements
5.15 Access control	possible		— Rules for controlling the physical and logical access to information and other associated assets, e.g. in a topic-specific policy on access control — Extracts (samples) of access rights for high-risk physical or logical access to information and other assets, checked for conformity to above rules
5.16 Identity management			— Procedures for managing identities assigned to persons or non-human entities over the life cycle
5.17 Authentication information	recommended		— Description of a process for allocation and management of authentication information — Instructions for users for proper handling of information used for authentication — Where passwords are used, security settings (e.g. length, complexity, rotation) of password management systems
5.18 Access rights	recommended		— Rules for access control, e.g. in a topic-specific policy on access control (physical and logical) — Description of process for assigning, updating or revoking access rights — Rules and process for regular review of access rights — Access rights assigned to a sample of identities — Results of performed reviews of access rights
5.19 Information security in supplier relationships			— Rules for managing the information security risks in supplier relationships, e.g. in a topic-specific policy on the use of supplier's products and services — Processes or procedures for managing information security in supplier relationships throughout the life cycle of the relationships — Results from supplier evaluations [e.g. Information and Communication Technology (ICT) infrastructure components, services] — Results from the monitoring of conformance to established information security requirements (e.g. for a sample of supplier relationships)

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
5.20 Addressing information security within supplier agreements			— Register of agreements with external parties, related to the type of supplier relationship — Supplier agreements (sample) with relevant information security requirements and Service Level Agreements
5.21 Managing information security in the information and communication technology (ICT) supply chain			— Rules for handling information security in ICT product or service acquisition — ICT supply chain information security risk management practices — Results of risk analysis performed, i.e. mitigating controls for sample of specific ICT supply chains
5.22 Monitoring, review and change management of supplier services			— Processes for managing changes in supplier information security practices and services delivery — Plans for regular monitoring, reviewing, evaluating supplier information security practices (e.g. through service reports, audits of suppliers) — Results from monitoring and review activities including action plans
5.23 Information security for use of cloud services			— Rules for managing the information security risks in cloud services, e.g. in a topic-specific policy on the use of cloud services — List of cloud services in use by the organization — Processes for managing information security risks associated with the use of cloud services — Specific provisions for the protection of the organization's data and availability of services, if the cloud service agreements do not cover the organization's confidentiality, integrity, availability and information handling requirement
5.24 Information security incident management planning and preparation			— Processes, plan, roles and responsibilities for handling information security incidents — Reporting procedures for information security events and examples of such reports
5.25 Assessment and decision on information security events			— Criteria for assessing information security events — Categorization and prioritization scheme for information security incidents
5.26 Response to information security incidents			— Procedures for information security incident response — Records of incidents and corresponding incident responses
5.27 Learning from information security incidents			— Records of information security incidents that occurred, including types, volumes and costs incurred — Lessons learned from the analysis of information security incidents, e.g. enhancements of incident management plan, improvement of controls and awareness activities
5.28 Collection of evidence			— Procedures for dealing with evidence related to information security incidents, e.g. for identification, collection, acquisition and preservation

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
5.29 Information security during disruption			— Plans for maintaining appropriate information security levels during disruption — Inclusion of information security requirements into the business continuity management planning and process
5.30 ICT readiness for business continuity			— ICT continuity requirements derived from business impact analysis — ICT continuity plans — Results of regular ICT continuity tests
5.31 Legal, statutory, regulatory and contractual requirements			— List of relevant countries which the organization conducts business in, or uses products and services of, which can affect the information security of the organization — Identified external requirements including legal, regulatory or contractual requirements relevant to information security, in particular, regarding the use of cryptography in any form
5.32 Intellectual property rights			— Rules for managing intellectual property rights, e.g. in a topic-specific policy — Procedures for handling document copyright, design rights, trademarks, patents and source code licences and corresponding inventories
5.33 Protection of records	recommended		— Rules for records management linked to the applicable laws, regulations and contractual requirements, e.g. in a topic-specific policy — Procedures on the storage, handling the chain of custody, retention and disposal of records — Configuration of data storage systems to enable requirements for records management (e.g. preservation, retention)
5.34 Privacy and protection of personal identifiable information (PII)			— Rules for handling personally identifiable information (PII), e.g. in a topic-specific policy — List of relevant countries which the organization conducts business in, or uses products and services of, that can affect privacy and protection of PII — Identified external requirements including legal, regulatory or contractual requirements for the preservation of privacy and protection of PII — Analyses performed by parties responsible for handling PII that show that requirements are met through appropriate technical and organizational measures
5.35 Independent review of information security			— Plans for conducting independent information security reviews — Reporting of results of the independent reviews (sample) to top management — Corrective actions taken where the organization's approach to managing information security was found to be inadequate

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
5.36 Compliance with policies, rules and standards for information security			— Plans for reviewing the organization's compliance with the information security policy, topic-specific policies, rules and standards — Results of such reviews (sample) and corrective actions taken
5.37 Documented operating procedures			— Operating procedures for information processing facilities, as relevant for information security
6 People controls			
6.1 Screening			— Rules and process for background checks, taking into consideration applicable laws, regulations and ethics — Background checks performed for sample of new entrants and current personnel as applicable (e.g. promotions, sensitive job profiles)
6.2 Terms and conditions of employment			— General rules or general terms and conditions related to information security responsibilities, e.g. code of conduct — Acceptance of terms and conditions concerning information security by personnel — Sample of specific information security responsibilities agreed by personnel with critical roles (e.g. having access to sensitive information or privileged access to systems)
6.3 Information security awareness, education and training			— Information security awareness, education and training programme including specific contents for important target groups — Attendance list for information security trainings performed — Responses from interviews with a sample of attendees on expected behaviours
6.4 Disciplinary process			— Formal disciplinary process, as communicated to personnel and other relevant interested parties
6.5 Responsibilities after termination or change of employment			— Signed acceptance by personnel of specific responsibilities and duties valid after leaving the company or after change of employment
6.6 Confidentiality or non-disclosure agreements			— Signed confidentiality agreements by personnel and other relevant interested parties
6.7 Remote working	possible		— Rules on working remotely, e.g. in a topic-specific policy — Samples of physical and communication security measures — Design of secure information processing devices permitted to use remotely [e.g. “Bring your own device” (BYOD), laptops]
6.8 Information security event reporting			— Mechanism for reporting information security events that can be identified by personnel — Instructions or communications to raise awareness on the reporting of information security events

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/ IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
7 Physical controls			
7.1 Physical security perimeters		possible	— Rules for construction of secure areas and for strengths of physical barriers — Physical security perimeter and secure area design for each relevant location
7.2 Physical entry	possible	recommended	— Access authorization system (physical or electronic) for entry points to secure areas — Logs of access for tracking entry of personnel and visitors — Physical design of delivery and loading areas with corresponding process descriptions
7.3 Securing offices, rooms and facilities		possible	— Physical security design and implementation of offices and facilities for shielding sensitive information being processed
7.4 Physical security monitoring	possible	possible	— Design of physical surveillance systems to detect unauthorized physical access — Protection of monitoring systems — Logs generated by the operation of physical surveillance systems
7.5 Protecting against physical and environmental threats		recommended	— Outcome of risk assessments on physical and environmental threats — Design of appropriate measures protecting against physical and environmental threats
7.6 Working in secure areas		possible	— Rules for working in secure areas (stating specific security measures) — Implemented security measures for secure areas
7.7 Clear desk and clear screen		recommended	— Rules for clear desk and clear screen, e.g. in a topic-specific policy — Spot checks on clear desk and clear screen behaviours (e.g. work areas and printers)
7.8 Equipment siting and protection		possible	— Rules for equipment siting and protection — Spot checks on equipment siting and protection
7.9 Security of assets off-premises			— Rules for use of assets outside organization's premises (e.g. BYOD guidelines) — Results of interviews or surveys performed among personnel using assets outside organization's premises
7.10 Storage media	possible		— Rules for use of removable storage media, e.g. in a topic-specific policy — Device configurations to restrict or protect transfer of information from and to removable storage media (including e.g. encryption) — Processes for secure disposal, and records from such processes

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
7.11 Supporting utilities		recommended	— Installed utility protection measures, especially in data centres (e.g. temperature, electric supply, water) — Emergency provisions to cut of power, water, gas or other utilities
7.12 Cabling security		possible	— Physical routing and protection of cabling
7.13 Equipment maintenance			— Procedures for maintenance of different types of equipment — Equipment maintenance records
7.14 Secure disposal or re-use of equipment	possible	possible	— Rules for disposal or re-use of equipment containing storage media — Records of physical or logical destruction of information or equipment
8 Technological controls			
8.1 User endpoint devices	possible		— Rules on secure configuration and handling of user endpoint devices, e.g. in a topic-specific policy — End-user awareness activities covering security requirements and procedures for protecting user endpoint devices — Rules on separation and protection of business information on private devices (BYOD), if applicable — Design of secure information processing devices permitted to use remotely (e.g. BYOD, laptops)
8.2 Privileged access rights	possible		— Rules on the restricted allocation, use and monitoring of privileged access rights, e.g. in a topic-specific policy — Authorization and review processes to manage privileged access rights
8.3 Information access restriction	recommended		— Rules on the restrictions of access to information and other associated assets, e.g. in a topic-specific policy — Access management techniques and processes to protect access to sensitive information throughout its life cycle (i.e. creation, processing, storage, transmission, disposal)
8.4 Access to source code	recommended		— Procedures for managing read and write access to source code, development tools and software libraries
8.5 Secure authentication	recommended		— Rules on authentication technologies and procedures for access control, e.g. in a topic-specific policy — Risk based decisions and corresponding implementations of log-on procedures for systems or applications — Use of strong or multi-factor authentication for critical information systems

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
8.6 Capacity management	possible		— Current and expected capacity requirements — Measurements of the use of resources, e.g. information processing facilities, human resources, offices and other facilities — Procedures for either providing sufficient capacity or reducing capacity requirements
8.7 Protection against malware	recommended		— Rules for protection against malware — Risk based coverage of assets and corresponding configuration of malware detection software — Other procedures and measures to protect information and other resources against malware — End-user awareness activities with regard to malware
8.8 Management of technical vulnerabilities	recommended		— Collection and management of information about technical vulnerabilities of information systems in use — Results of vulnerability scans (regularly performed) or from penetration tests — Evaluations performed of the organization's exposure to technical vulnerabilities and planned mitigating measures — Software update process to ensure installation of most up-to-date approved patches and application updates
8.9 Configuration management	recommended		— Rules on the configurations, including security configurations, of hardware, software, services and networks — Processes for managing, implementing or applying, monitoring and reviewing configurations — Standard templates for the secure configuration of hardware, software, services and networks (i.e. hardening)
8.10 Information deletion			— Rules for the timely deletion of information stored in information systems, devices or in any other storage media, e.g. according to a topic-specific policy on data retention — Procedures for securely deleting sensitive information on systems, applications and services — Third-party agreements with provisions for information deletion, where third parties store the organization's information
8.11 Data masking			— Rules on data masking, e.g. according to the organization's topic-specific policy on access control — Results of analyses performed to determine where the protection of sensitive information (e.g. PII) requires techniques such as data masking, pseudonymization or anonymization — Techniques used for data masking, pseudonymization or anonymization

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/ IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
8.12 Data leakage prevention	possible		— Rules on data leakage prevention measures to be applied to systems, networks and any other devices that process, store or transmit sensitive information — Identified information requiring protection against leakage — Identified relevant leakage channels with measures to prevent leakage including monitoring — Configuration of data loss prevention system
8.13 Information backup	recommended		— Rules on the backup of information, software and systems, e.g. in a topic-specific policy on backup — Backup plans, based on established business requirements of the organization — Operational procedures for monitoring the timely and correct execution of backups and to address failures — Backup restoration tests performed at regular intervals
8.14 Redundancy of information processing facilities			— Identified requirements for the availability of business services and information systems — Architecture of systems with high requirements providing appropriate redundancy — Results of failover tests performed
8.15 Logging	recommended		— Rules on the purpose for which logs are created, what data are collected, and any log-specific requirements for handling the log data, e.g. in a topic-specific policy on logging — List of security-relevant logs and measures to ensure their protection against unauthorized manipulations — Procedures for performing regular analysis and interpretation of log events, e.g. to identify unusual activities or anomalous behaviour — Configuration of log systems
8.16 Monitoring activities	possible		— Rules for monitoring of networks, systems and applications for anomalous behaviour — Established baselines of normal behaviour and derived criteria for triggering alerts — Monitoring logs maintained for defined retention periods — Results of analysis performed to identify anomalous behaviour
8.17 Clock synchronization	possible		— List of reference time sources used by the organization — Clock synchronization methods and handling of time differences

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
8.18 Use of privileged utility programs	possible		— List of utility programs used that may be capable of overriding system and application controls — Processes, procedures and other methods used to restrict and tightly control such utility programs
8.19 Installation of software on operational systems	possible		— Procedures and measures used for managing installation of software on operational systems, including inventories of installed software with versions — Rules on which types of software users can install — Restrictions for installing software by persons other than trained administrators
8.20 Networks security	recommended		— Rules for ensuring the security of information in networks and to protect connected services from unauthorized access — Measures and security features implemented to protect information in networks and its supporting information processing facilities, e.g. configuration templates, configuration of cryptographic controls, rulesets of gateways, sample of configuration of network devices — Network architecture documentation (diagrams, configuration files, segregation) — Rules for authenticating systems connections to the network
8.21 Security of network services			— Rules on the secure use of networks and network services — List of networks and network services used with security mechanisms and service levels — Assurance obtained from network service providers
8.22 Segregation of networks			— Rules on segregation of network domains based e.g. on levels of trust, criticality and sensitivity and according to the topic-specific policy on access control — Network topology (including wireless) and segregation of zones with description of purpose and rules — Definitions of security perimeters of network domains — Processes to manage security perimeters of network domains, as well as firewall rules
8.23 Web filtering	possible		— Rules on the safe and appropriate use of online resources, including any restrictions to undesirable or inappropriate websites — Measures implemented to reduce the exposure to malicious content of external websites, e.g. filtering rules — Awareness and training activities delivered to all personnel on the secure and appropriate use of online resources

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/ IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
8.24 Use of cryptography	recommended		— Rules for the effective use of cryptography, including acceptable ciphers and key management, e.g. in a topic-specific policy on cryptography — List of cryptographic techniques in use by the organization — Standards, procedures and methods for key management, including generating, storing, archiving, retrieving, distributing, retiring and destroying cryptographic keys
8.25 Secure development life cycle	possible		— Rules on secure software development to ensure information security is designed and implemented within the secure development life cycle — Separation between development, test and production environments — Security processes and checkpoints ensuring adequate covering of information security requirements during the entire software development — Assurance obtained on the appropriate handling of information security requirements where software development is outsourced
8.26 Application security requirements			— Process for defining application security requirements based on specific risk assessment — Application risk assessments performed, stating the specific information security requirements — Requirements identified for a sample of recent developments/implementations of applications, in particular for transactional services, electronic ordering and payment applications
8.27 Secure system architecture and engineering principles			— Architecture and security engineering principles established to ensure that information systems are security designed, implemented and operated within the development life cycle — Integration of security engineering principles in software development — Sample of application-specific security implementation confirming the use of the above engineering principles — Embedded secure engineering principles in contracts for outsourced development, if applicable
8.28 Secure coding	possible		— Rules on secure coding principles used both for new developments and in reuse scenarios — Processes for ensuring the application of secure coding principles during planning and before coding, during coding, and during review and maintenance — Application of specific secure coding principles for samples of recent development activities, including code scanning techniques — Protection mechanisms for code, including access restrictions

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Table E.1 *(continued)*

Controls in ISO/IEC 27001:2022, Annex A [a]	System testing	Visual inspection	Possible evidence of design and implementation of controls
8.29 Security testing in development and acceptance	recommended		— Rules on security testing to validate if information security requirements are met when applications or code are deployed to the production environment — Samples of sets of requirements actually used for security testing and corresponding test results — Output and follow-up from automated test tools (e.g. code analysis tools, vulnerability scanners, functional tests)
8.30 Outsourced development			— Rules on how information security measures required by the organization shall be implemented in outsourced system development — Procedures implemented to direct, monitor and review the activities related to outsourced system development — Outcome of monitoring or review of suppliers to ensure expectations are met
8.31 Separation of development, test and production environments	possible		— Rules for the level of separation between production, testing and development environments, including specific requirements for the different development environments — Separation between development, test and production environments — Protection of test and production environments (e.g. access restrictions, network segregation, ensuring no sensitive production information is used)
8.32 Change management	recommended		— Rules for managing changes to preserve information security — Change control procedures, e.g. documentation, specification, testing, quality control and managed implementation — Sample of changes performed showing how changes were tested, approved and deployed
8.33 Test information	possible		— Rules on the appropriate selection, use, protection and management of test information — Procedures for protection of operational information, during their use for testing purposes (e.g. masking) — Samples of deletion of information from test environments
8.34 Protection of information systems during audit testing	possible		— List of requests for audit tests or other assurance activities involving assessment of operational systems — Sample of performed audit tests and how these were agreed and conducted

[a] The numbers cited in this column correspond to the control numbers in ISO/IEC 27001:2022, Annex A.

Bibliography

[1] ISO 19011, *Guidelines for auditing management systems*

[2] ISO/IEC 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

[3] ISO/IEC 27002, *Information security, cybersecurity and privacy protection — Information security controls*

[4] ISO/IEC 27006-2, *Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems — Part 2: Privacy information management systems*

[5] ISO/IEC 27007, *Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*

[6] ISO 9000, *Quality management systems — Fundamentals and vocabulary*

[7] ISO 9001, *Quality management systems — Requirements*

[8] ISO Guide 73[1)], *Risk management — Vocabulary*

[9] IAF MD5 *Determination of Audit Time of Quality, Environmental, and Occupational Health & Safety Management Systems*, https://iaf.nu/en/iaf-documents/?cat_id=7, Last viewed: 2023-07-31.

1) Withdrawn.

ICS 35.030; 03.120.20

Price based on 47 pages

iso.org