FINAL
DRAFT

INTERNATIONAL
STANDARD

**ISO/IEC
FDIS
27006-1**

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2023-11-02

Voting terminates on:
2023-12-28

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

Part 1: General

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/IEC FDIS 27006-1:2023(E)

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 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;