SLOVENSKI STANDARD
oSIST prEN ISO/IEC 27006-1:2022

01-september-2022

Zahteve za organe, ki izvajajo presojanje in certificiranje sistemov upravljanja informacijske varnosti - 1. del: Splošno (ISO/IEC/DIS 27006-1:2022)

Requirements for bodies providing audit and certification of information security management systems - Part 1: General (ISO/IEC/DIS 27006-1:2022)

Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren - Teil 1: Allgemeines (ISO/IEC/DIS 27006-1:2022)

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 (ISO/IEC/DIS 27006-1:2022)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 27006-1**

ICS:

03.120.20	Certificiranje proizvodov in podjetij. Ugotavljanje skladnosti	Product and company certification. Conformity assessment
35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 27006-1:2022 **en,fr,de**

DRAFT INTERNATIONAL STANDARD
ISO/IEC DIS 27006-1

ISO/IEC JTC **1**/SC **27**
Secretariat: **DIN**

Voting begins on:
2022-07-01

Voting terminates on:
2022-09-23

Requirements for bodies providing audit and certification of information security management systems —

Part 1:
General

ICS: 35.030; 03.120.20

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/IEC DIS 27006-1:2022(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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *Information security, cybersecurity and privacy protection*.

ISO/IEC 27006-1 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This document cancels and replaces the second edition (ISO/IEC 27006:2015), which has been technically revised. It has been renumbered and so is the first edition of ISO/IEC 27006-1.

Introduction

ISO/IEC 17021-1 sets out criteria for bodies operating audit and certification of management systems. If such bodies are to be accredited as complying with ISO/IEC 17021-1 with the objective of auditing and certifying information security management systems (ISMS) in accordance with ISO/IEC 27001:2013 and possibly sector-specific standard extensions of ISO/IEC 27001, some additional requirements and guidance to ISO/IEC 17021-1 are necessary. These are provided by this Document.

The text in this Document follows the structure of ISO/IEC 17021-1 and the additional ISMS-specific requirements and guidance on the application of ISO/IEC 17021-1 for ISMS certification are identified by the letters "IS".

The term "shall" is used throughout this Document to indicate those provisions which, reflecting the requirements of ISO/IEC 17021-1 and ISO/IEC 27001, are mandatory. The term "should" is used to indicate recommendation.

The primary purpose of this Document is to enable accreditation bodies to more effectively harmonize their application of the standards against which they are bound to assess certification bodies.

Throughout this Document, the terms "management system" and "system" are used interchangeably. The definition of a management system can be found in ISO 9000:2005. The management system as used in this Document is not to be confused with other types of systems, such as IT systems.

The certification body may offer audit and certification services to sector-specific standard extensions of ISO/IEC 27001 in addition to audit and certification to ISO/IEC 27001.

NOTE The extension of ISO/IEC 7001 through the application of a sector-specific standard does not result in a management system independent of the ISMS.

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. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.

The requirements contained in this document need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in this document provides additional interpretation of these requirements for any body 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, in whole or in part, are normatively referenced in this document and are indispensable for its application. 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 27001:2013, *Information technology — Security techniques — 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.

3.1
certification documents
documents indicating that a client's ISMS conforms to specified ISMS standards and any supplementary documentation required under the system

3.2
sector-specific standard
standard that extends Annex A of ISO/IEC 27001 to support a specific sector

Note 1 to entry: A sector specific standard provides additions to the controls in ISO/IEC 27002 or provides guidance on which elements to consider in the organizational context, interested parties, their needs and expectations to implement the requirements in ISO/IEC 27001 or guidance on the implementation of controls.

Note 2 to entry: A sector specific extension standard of ISO/IEC 27001 doesn't change the requirements of ISO/IEC 27001, including any addition and modification.

3.3
control
measure that is modifying risk (3.10)

Note 1 to entry: Controls include any process, policy, device, practice, or other actions which modify risk (3.10).

Note 2 to entry: It is possible that controls not always exert the intended or assumed modifying effect.

[SOURCE: ISO/IEC 27000:2018, 3.14]

3.4
control objective
statement describing what is to be achieved as a result of implementing controls (3.3)

[SOURCE: ISO/IEC 27000:2018, 3.15]

3.5
external context
external environment in which the organization 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;

— relationships with, and perceptions and values of, external stakeholders.

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

3.6
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]

3.7
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 (3.6)

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

3.8
information system
set of applications, services, information technology assets, or other information-handling components

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

3.9
internal context
internal environment in which the organization 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, information flows and decision-making processes (both formal and informal);

— relationships with, and perceptions and values of, internal stakeholders;

— the organization's culture;

— standards, guidelines and models adopted by the organization;

— form and extent of contractual relationships.

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

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 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.

[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 (3.11) provides the basis for risk evaluation and decisions about risk treatment (3.14).

Note 2 to entry: Risk analysis (3.11) 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 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.

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

4 Principles

The principles from ISO/IEC 17021-1, 4 apply.

5 General requirements

5.1 Legal and contractual matters

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

5.2 Management of impartiality

The requirements of ISO/IEC 17021-1, 5.2 apply. In addition, the following requirements and guidance apply.

5.2.1 IS 5.2 Conflicts of interest

Certification bodies may carry out the following duties without them being considered as consultancy or having a potential conflict of interest:

a) arranging and participating as a lecturer in training courses, provided that, where these courses relate to information security management, related management systems or auditing, certification bodies shall confine themselves to the provision of generic information and advice which is publicly available, i.e. they shall not provide company-specific advice;

b) making available or publishing on request information describing the certification body's understanding of the requirements of the certification audit standards;

c) activities prior to audit, solely aimed at determining readiness for certification audit; however, such activities shall not result in the provision of recommendations or advice that would contravene this clause and the certification body shall be able to confirm that such activities do not contravene these requirements and that they are not used to justify a reduction in the eventual certification audit duration;

d) performing second and third-party audits according to standards or regulations other than those being part of the scope of accreditation;

e) adding value during certification and surveillance audits, e.g. by identifying opportunities for improvement, as they become evident during the audit, without recommending specific solutions.

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, 5.3 apply.

6 Structural requirements

The requirements of ISO/IEC 17021-1, 6 apply.

7 Resource requirements

7.1 Competence of personnel

The requirements of ISO/IEC 17021-1, 7.1 apply. In addition, the following requirements and guidance apply.

7.1.1 IS 7.1.1 General considerations

7.1.1.1 Generic competence requirements

The certification body shall ensure that it has knowledge of the technological, legal and regulatory developments relevant to the ISMS of the client which it assesses.

The certification body shall define the competence requirements for each certification function as referenced in Table A.1 of ISO/IEC 17021-1. The certification body shall take into account all the requirements specified in ISO/IEC 17021-1 and 7.1.2 and 7.2.1 of this document that are relevant for the ISMS technical areas as determined by the certification body.

NOTE Annex A provides a summary of the competence requirements for personnel involved in specific certification functions. For sector-specific competency requirements, refer the related part of the ISO/IEC 27006 series (for example, ISO/IEC 27006-2 for privacy information management systems).

If no applicable part of the ISO/IEC 27006 series exists, the certification body shall define competence requirements for each certification function for activities that include the sector-specific standard(s) extending the audit criteria.

7.1.2 IS 7.1.2 Determination of Competence Criteria

7.1.2.1 Competence requirements for ISMS auditing

7.1.2.1.1 General requirements

The certification body shall have criteria for verifying the background experience, specific training or briefing of audit team members that ensures at least:

a) knowledge of information security;

b) technical knowledge of the activity to be audited;

c) knowledge of management systems;

d) knowledge of the principles of auditing;

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

e) knowledge of ISMS monitoring, measurement, analysis and evaluation.

These above requirements a) to e) apply to all auditors being part of the audit team, with the exception of b), which can be shared among auditors being part of the audit team.

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

The audit team members shall, collectively, have appropriate work experience of the items above and practical application of these items (this does not mean that an auditor needs a complete range of experience of all areas of information security, but the audit team as a whole shall have enough appreciation and experience to cover the ISMS scope being audited).

7.1.2.1.2 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 may be relevant or an issue.

7.1.2.1.3 Information security management system standards and normative documents

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

a) all requirements contained in ISO/IEC 27001.

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

b) all controls contained in ISO/IEC 27002 (and, if applicable, relevant sector-specific standards) and their implementation.

7.1.2.1.4 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 inter-relationship 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.

7.1.2.1.5 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 amongst the audit team.

7.1.2.1.6 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.

7.1.2.2 Competence requirements for conducting the application review

7.1.2.2.1 Information security management system standards and normative documents

Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of:

a) relevant ISMS standards and other normative documents used in the certification process.

7.1.2.2.2 Client business sector

Personnel conducting the application review to determine the audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of:

a) generic terminology, processes, technologies and risks related to the client business sector.

7.1.2.2.3 Client products, processes and organization

Personnel conducting the application review to determine audit team competence required, to select the audit team members and to determine the audit time shall have knowledge of:

a) 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 outsourcing functions.

7.1.2.3 Competence requirements for reviewing audit reports and making certification decisions

7.1.2.3.1 General

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