SLOVENSKI STANDARD

oSIST prEN ISO/IEC 27006:2020

01-oktober-2020

Informacijska tehnologija - Varnostne tehnike - Zahteve za organe, ki izvajajo presojanje in certificiranje sistemov upravljanja informacijske varnosti (ISO/IEC 27006:2015, vključno z dopolnilom 1:2020)

Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems (ISO/IEC 27006:2015, including Amd 1:2020)

Informationstechnik - IT-Sicherheitsverfahren - Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managmentsystemen anbieten (ISO/IEC 27006:2015, einschließlich Amd 1:2020)

Technologies de l'information - Techniques de sécurité - Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information (ISO/IEC 27006:2015, y compris Amd 1:2020)

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

ICS:

03.100.70	Sistemi vodenja	Management systems
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 27006:2020 **en,fr,de**

INTERNATIONAL STANDARD

ISO/IEC 27006

Third edition
2015-10-01

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Reference number
ISO/IEC 27006:2015(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

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, *IT Security techniques*.

ISO/IEC 27006 was prepared by the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 27006:2011), which has been technically revised.

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, some additional requirements and guidance to ISO/IEC 17021-1 are necessary. These are provided by this International Standard.

The text in this International Standard 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 International Standard 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 International Standard 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 International Standard, 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 International Standard is not to be confused with other types of systems, such as IT systems.

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

1 Scope

This International Standard 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 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification.

The requirements contained in this International Standard need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in this International Standard provides additional interpretation of these requirements for any body providing ISMS certification.

NOTE This International Standard 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 27000, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*

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, ISO/IEC 27000 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

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 which contravenes the requirements of b) below;

b) making available or publishing on request information describing the certification body's interpretation of the requirements of the certification audit standards (see 9.1.3.6);

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 audits and surveillance visits, 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 International Standard 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.

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 shall 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 shall 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

Collectively, all members of the audit team shall have knowledge of:

a) ISMS specific documentation structures, hierarchy and interrelationships;

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

c) information security risk assessment and risk management;

d) processes applicable to ISMS;

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

Every auditor shall fulfil a), c) and d).

7.1.2.1.3 Information security management system standards and normative documents

Auditors involved in ISMS auditing shall have knowledge of:

a) all requirements contained in ISO/IEC 27001.

Collectively, all members of the audit team shall have knowledge of:

b) all controls contained in ISO/IEC 27002 (if determined as necessary also from sector specific standards) and their implementation, categorized as:

   1) information security policies;

   2) organization of information security;

   3) human resource security;

   4) asset management;

   5) access control, including authorization;

   6) cryptography;

   7) physical and environmental security;

   8) operations security, including IT-services;

   9) communications security, including network security management and information transfer;

   10) system acquisition, development and maintenance;

   11) supplier relationships, including outsourced services;

   12) information security incident management;

   13) information security aspects of business continuity management, including redundancies;

   14) compliance, including information security reviews.

7.1.2.1.4 Business management practices

Auditors involved in ISMS auditing 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

Auditors involved in ISMS auditing 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 criteria a) may be shared amongst the audit team.

7.1.2.1.6 Client products, processes and organization

Collectively, auditors involved in ISMS auditing shall 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 leading the ISMS audit team

In addition to the requirements in 7.1.2.1, audit team leaders shall fulfil the following requirements, which shall be demonstrated in audits under guidance and supervision:

a) knowledge and skills to manage the certification audit process and the audit team;

b) demonstration of the capability to communicate effectively, both orally and in writing.

7.1.2.3 Competence requirements for conducting the application review

7.1.2.3.1 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.

7.1.2.3.2 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.

7.1.2.3.3 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) client products, processes, organization types, size, governance, structure, functions and relationships on development and implementation of the ISMS and certification activities, including outsourcing functions.