Information security, cybersecurity and privacy protection - Requirements for bodies providing audit and certification of information security management systems - Part 1: General (ISO/IEC 27006-1:2024)

EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 27006-1:2024 sisaldab Euroopa standardi EN ISO/IEC 27006-1:2024 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 27006-1:2024 consists of the English text of the European standard EN ISO/IEC 27006-1:2024.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 13.03.2024.	Date of Availability of the European standard is 13.03.2024.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile standardiosakond@evs.ee.

ICS 03.120.20, 35.030

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 27006-1

March 2024

ICS 03.120.20; 35.030

Supersedes EN ISO/IEC 27006:2020

English version

Information security, cybersecurity and privacy protection - Requirements for bodies providing audit and certification of information security management systems - Part 1: General (ISO/IEC 27006-1:2024)

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 (ISO/IEC 27006-1:2024)

Cybersicherheit und Datenschutz - Anforderungen an Stellen, die Informationssicherheitsmanagementsysteme auditieren und zertifizieren - Teil 1: Allgemeines (ISO/IEC 27006-1:2024)

This European Standard was approved by CEN on 29 January 2024.

This European Standard was corrected and reissued by the CEN-CENELEC Management Centre on 20 March 2024.

European foreword

This document (EN ISO/IEC 27006-1:2024) has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" in collaboration with Technical Committee CEN-CENELEC/ JTC 13 “Cybersecurity and Data Protection” the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by September 2024, and conflicting national standards shall be withdrawn at the latest by September 2024.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 27006:2020.

Any feedback and questions on this document should be directed to the users’ national standards body/national committee. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 27006-1:2024 has been approved by CEN-CENELEC as EN ISO/IEC 27006-1:2024 without any modification.

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Principles **4**
5 General requirements **5**
5.1 Legal and contractual matters 5
5.2 Management of impartiality 5
5.2.1 General 5
5.2.2 Conflicts of interest 5
5.3 Liability and financing 5
6 Structural requirements **5**
7 Resource requirements **5**
7.1 Competence of personnel 5
7.1.1 General 5
7.1.2 Generic competence requirements 5
7.1.3 Determination of competence criteria 6
7.2 Personnel involved in the certification activities 8
7.2.1 General 8
7.2.2 Demonstration of auditor knowledge and experience 8
7.3 Use of individual external auditors and external technical experts 9
7.4 Personnel records 9
7.5 Outsourcing 9
8 Information requirements **9**
8.1 Public information 9
8.2 Certification documents 9
8.2.1 General 9
8.2.2 ISMS Certification documents 10
8.2.3 Reference of other standards in the ISMS certification documents 10
8.3 Reference to certification and use of marks 10
8.4 Confidentiality 10
8.4.1 General 10
8.4.2 Access to organizational records 10
8.5 Information exchange between a certification body and its clients 10
9 Process requirements **11**
9.1 Pre-certification activities 11
9.1.1 Application 11
9.1.2 Application review 11
9.1.3 Audit programme 11
9.1.4 Determining audit time 12
9.1.5 Multi-site sampling 13
9.1.6 Multiple management systems 14
9.2 Planning audits 14
9.2.1 Determining audit objectives, scope and criteria 14
9.2.2 Audit team selection and assignments 14
9.2.3 Audit plan 15
9.3 Initial certification 15
9.3.1 General 15
9.3.2 Initial certification audit 15
9.4 Conducting audits 16

9.4.1 General ... 16
9.4.2 Specific elements of the ISMS audit ... 16
9.4.3 Audit report ... 16
9.5 Certification decision ... 17
9.5.1 General ... 17
9.5.2 Certification decision ... 17
9.6 Maintaining certification ... 17
9.6.1 General ... 17
9.6.2 Surveillance activities ... 17
9.6.3 Re-certification ... 18
9.6.4 Special audits ... 18
9.6.5 Suspending, withdrawing or reducing the scope of certification ... 18
9.7 Appeals ... 19
9.8 Complaints ... 19
9.8.1 General ... 19
9.8.2 Complaints ... 19
9.9 Client records ... 19

10 Management system requirements for certification bodies ... 19
10.1 Options ... 19
10.1.1 General ... 19
10.1.2 ISMS implementation ... 19
10.2 Option A: General management system requirements ... 19
10.3 Option B: Management system requirements in accordance with ISO 9001 ... 19

Annex A (normative) **Knowledge and skills for ISMS auditing and certification ... 20**

Annex B (informative) **Further competence considerations ... 21**

Annex C (normative) **Audit time ... 23**

Annex D (informative) **Methods for audit time calculations ... 29**

Annex E (informative) **Guidance for review of implemented ISO/IEC 27001:2022, Annex A controls ... 33**

Bibliography ... 47

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.