



**Irish Standard**  
**I.S. EN ISO/IEC 27006-1:2024**

**Version 1.0**

**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)**

**I.S. EN ISO/IEC 27006-1:2024 V1.0****The National Standards Authority of Ireland (NSAI) produces the following categories of formal documents:**

I.S. xxx: Irish Standard — national specification based on the consensus of an expert panel and subject to public consultation.

S.R. xxx: Standard Recommendation — recommendation based on the consensus of an expert panel and subject to public consultation.

SWiFT xxx: A rapidly developed recommendatory document based on the consensus of the participants of an NSAI workshop.

NSAI/... xxx: A National adoption of a Technical Regulation (TR), Technical Specification (TS), CEN and/or CENELEC Workshop Agreement (CWA).

I.S. EN ISO/IEC 27006-1:2024 V1.0 was published under the authority of the NSAI and came into effect on:				2024-03-14
Consisting of:	DAV	Version	Published	Withdrawn*
I.S. EN ISO/IEC 27006-1:2024	2024-03-13	1.0	2024-03-14	
Replaces:				
EN ISO	All versions			
*Dates in the future are planned withdrawal dates				
DAV = Date of Availability of publication from CEN/CENELEC				
NOTE 1: Versions relate to the different elements assembled for any publication based on the edition issued by CEN/CENELEC. Publications prior to 2023-11-27 do not contain version history but if you need any more information please contact <a href="mailto:info@standards.ie">info@standards.ie</a> .				
NOTE 2: The date of any NSAI previous adoptions may not match the date of its original CEN/CENELEC document.				

ICS number(s): 03.120.20, 35.030

NSAI  
1 Swift Square  
Northwood, Santry  
Dublin 9  
D09 A0E4  
+353 1 807 3800  
[standards@nsai.ie](mailto:standards@nsai.ie)  
[NSAI.ie](http://NSAI.ie)

Sales  
+353 1 857 6730  
[Standards.ie](http://Standards.ie)

Údarás um Chaighdeán Náisiúnta na hÉireann

## **National Foreword**

I.S. EN ISO/IEC 27006-1:2024 V1.0 is the version of the NSAI adopted European document EN ISO/IEC 27006-1:2024, *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)*, including any Corrections, Amendments etc. to EN ISO/IEC 27006-1:2024 listed on page(s) II.

This normative document by CEN/CENELEC the elaboration of which includes a public enquiry, followed by a Formal Vote of CEN/CENELEC national members and final ratification. This European Standard is published as an identical national standard and every conflicting national standard will be withdrawn. The content of a European Standard does not conflict with the content of any other EN (and HD for CENELEC).

This document does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

For relationships with other publications refer to the NSAI web store.

**Conformance with this document does not of its self confer immunity from legal obligations.**

In line with international standards practice the decimal point is shown as a comma (,) throughout this document.
---

This page intentionally left blank

EUROPEAN STANDARD

EN ISO/IEC 27006-1

NORME EUROPÉENNE

EUROPÄISCHE NORM

March 2024

ICS 03.120.20; 35.030

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.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of 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 United Kingdom.



CEN-CENELEC Management Centre:  
Rue de la Science 23, B-1040 Brussels

**I.S. EN ISO/IEC 27006-1:2024 V1.0**

**EN ISO/IEC 27006-1:2024 (E)**

<b>Contents</b>	<b>Page</b>
<b>European foreword.....</b>	<b>3</b>

## **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.

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.

This page intentionally left blank



## ISO/IEC 27006-1:2024(en)

## Contents

	Page
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 Principles</b> .....	<b>4</b>
<b>5 General requirements</b> .....	<b>5</b>
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
<b>6 Structural requirements</b> .....	<b>5</b>
<b>7 Resource requirements</b> .....	<b>5</b>
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
<b>8 Information requirements</b> .....	<b>9</b>
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
<b>9 Process requirements</b> .....	<b>11</b>
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
<b>10</b>	<b>Management system requirements for certification bodies</b>	<b>19</b>
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
	<b>Annex A (normative) Knowledge and skills for ISMS auditing and certification</b>	<b>20</b>
	<b>Annex B (informative) Further competence considerations</b>	<b>21</b>
	<b>Annex C (normative) Audit time</b>	<b>23</b>
	<b>Annex D (informative) Methods for audit time calculations</b>	<b>29</b>
	<b>Annex E (informative) Guidance for review of implemented ISO/IEC 27001:2022, Annex A controls</b>	<b>33</b>
	<b>Bibliography</b>	<b>47</b>

## ISO/IEC 27006-1:2024(en)

## 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://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.

This is a free preview. Purchase the entire publication at the link below:

[Product Page](#)

- 
- [Looking for additional Standards? Visit Intertek Inform Infostore](#)
  - [Learn about LexConnect, All Jurisdictions, Standards referenced in Australian legislation](#)
-