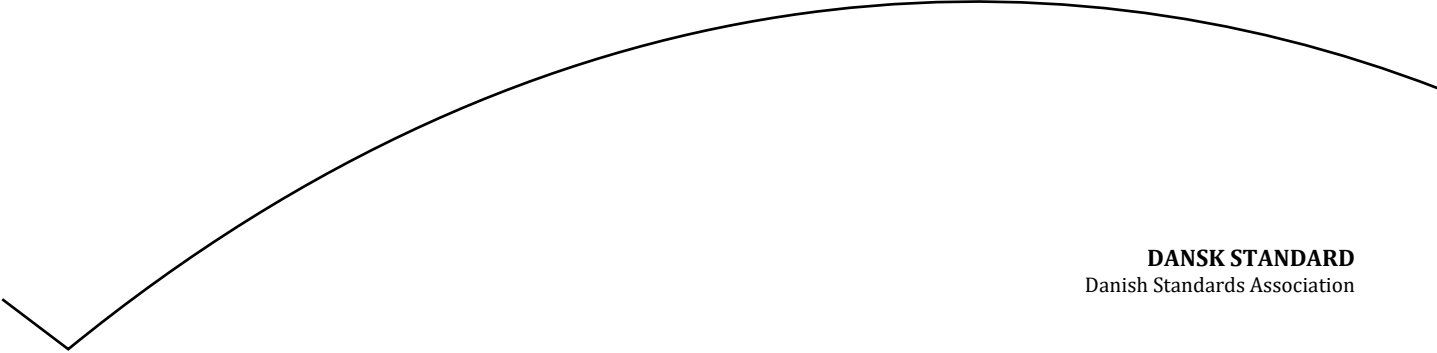


2026-06-16

Informationsteknologi, cybersikkerhed og privatlivsbeskyttelse – Krav til organer, der foretager audit og certificering af ledelsessystemer for informationssikkerhed – Del 1: Generelt

Information technology, cybersecurity and privacy protection
– Requirements for bodies providing audit and certification of
information security management systems – Part 1: General
(ISO/IEC/DIS 27006-1:2023)



DANSK STANDARD
Danish Standards Association

Göteborg Plads 1
DK-2150 Nordhavn

Tel: +45 39 96 61 01
dansk.standard@ds.dk

www.ds.dk

DS/EN ISO/IEC 27006-1:2024

København

DS projekt: M362704

ICS: 03.120.20

ICS: 35.030

Første del af denne publikations betegnelse er:

DS/EN ISO/IEC, hvilket betyder, at det er en international standard, der har status både som europæisk og dansk standard.

Denne publikations overensstemmelse er:

IDT med: EN ISO/IEC 27006-1:2024

IDT med: ISO/IEC 27006-1:2024

DS-publikationen er på engelsk.

Denne publikation erstatter: [DS/EN ISO/IEC 27006:2020](#)

I tilfælde af redaktionelle fejl i DS-publikationen kan der skrives til:

editorial-mistakes@ds.dk

ADVARSEL: DS-publikationer revideres over tid. Derudover kan sådanne publikationer ændres ved rettelsesblade og/eller tillæg. Der kan også udgives rettelsesblade, der udelukkende angår oversættelsen af en publikation. Det er derfor vigtigt at sikre sig, at man benytter en gældende udgave, medmindre fx lovgivning kræver andet. Den enkelte publikations status fremgår af <https://webshop.ds.dk/>. Her kan man desuden tilmelde sig en gratis notifikationservice og følge en udgivet DS-publikations udvikling ved at klikke på "Følg".

En oversigt over forskellige DS-publikationstyper og -betegnelser findes her:

<https://www.ds.dk/publikationstyper>

Indholdet i dette dokument er ophavsretligt beskyttet, herunder tekst, grafik, billeder og lyd. Fonden Dansk Standard forbeholder sig udtrykkeligt alle rettigheder til at udnytte indholdet til tekst- og datamining, jf. ophavsretslovens § 11 b, stk. 2, og artikel 4 i direktiv (EU) 2019/790. Enhver udnyttelse af indholdet i dette dokument til tekst- og dataminingformål kræver forudgående skriftlig, specifik tilladelse fra Fonden Dansk Standard.

In case of editorial errors in the DS publication, please write to:

editorial-mistakes@ds.dk

NOTICE: DS publications are revised over time. In addition, such publications may be altered by corrigenda and/or amendments. Also, corrigenda may be published solely in relation to the translation of a publication. It is therefore important to ensure that the edition used is valid, unless, for example, legislation requires otherwise. The status of each publication can be found at <https://webshop.ds.dk/>. Here you can also sign up for a free notification service and follow the progress of a published DS publication by clicking on "Follow".

An overview of different DS publication types and designations can be found here:

<https://www.ds.dk/publikationstyper>

The content of this document, including text, graphics, images, and audio, is protected by copyright. The Danish Standards Foundation explicitly reserves all rights regarding the use of its content for text and data mining purposes in accordance with Section 11b(2) of the Danish Copyright Act and Article 4 of Directive (EU) 2019/790. Any use of the content of this document for text and data mining purposes requires prior, written, specific permission from the Danish Standards Foundation.

EUROPÄISCHE NORM

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 Informationssicherheitsmanagement-
systeme 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

This is a preview of DS/EN ISO/IEC 27006-1:2024. [Click here to purchase the full version from the ANSI store.](#)

Contents

Page

European foreword.....	3
------------------------	---

This is a preview of DS/EN ISO/IEC 27006-1:2024. [Click here to purchase the full version from the ANSI store.](#)

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.

ISO/IEC 27006-1

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

Part 1: General

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

First edition
2024-03



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

This is a preview of DS/EN ISO/IEC 27006-1:2024. [Click here to purchase the full version from the ANSI store.](#)

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

This is a preview of DS/EN ISO/IEC 27006-1:2024. [Click here to purchase the full version from the ANSI store.](#)

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

This is a preview of DS/EN ISO/IEC 27006-1:2024. Click here to purchase the full version from the ANSI store.

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.

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.

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;

This is a preview of DS/EN ISO/IEC 27006-1:2024. Click [here](#) to purchase the full version from the ANSI store.

— 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]

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.]