

---

**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-Managementsystemen anbieten (ISO/IEC 27006:2015, einschließlich Amd 1:2020)

<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-90761877211/sist-en-iso-iec-27006-2021>

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: EN ISO/IEC 27006:2020**

---

**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

**SIST EN ISO/IEC 27006:2021**

**en,fr,de**

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN ISO/IEC 27006:2021](https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021)

<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021>

EUROPEAN STANDARD

EN ISO/IEC 27006

NORME EUROPÉENNE

EUROPÄISCHE NORM

November 2020

ICS 03.120.20; 35.030

English version

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

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

This European Standard was approved by CEN on 16 November 2020.

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, Turkey and United Kingdom.



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

Contents	Page
European foreword.....	3

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN ISO/IEC 27006:2021](https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021)  
<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021>

## European foreword

The text of ISO/IEC 27006:2015 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 27006:2020 by Technical Committee CEN/CLC/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 May 2021, and conflicting national standards shall be withdrawn at the latest by May 2021.

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

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, Turkey and the United Kingdom.

## iTeh STANDARD PREVIEW Endorsement notice (standards.iteh.ai)

The text of ISO/IEC 27006:2015 has been approved by CEN as EN ISO/IEC 27006:2020 without any modification.

[SIST EN ISO/IEC 27006:2021](https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021)

<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN ISO/IEC 27006:2021](#)

<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021>

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*

iTeh STANDARD PREVIEW  
(standards.iteh.ai)

SIST EN ISO/IEC 27006:2021

<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021>

---

---

Reference number  
ISO/IEC 27006:2015(E)



© ISO/IEC 2015

## iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO/IEC 27006:2021

<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021>



### **COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, 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  
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
<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>1</b>
<b>5 General requirements</b> .....	<b>2</b>
5.1 Legal and contractual matters.....	2
5.2 Management of impartiality.....	2
5.2.1 IS 5.2 Conflicts of interest.....	2
5.3 Liability and financing.....	2
<b>6 Structural requirements</b> .....	<b>2</b>
<b>7 Resource requirements</b> .....	<b>2</b>
7.1 Competence of personnel.....	2
7.1.1 IS 7.1.1 General considerations.....	3
7.1.2 IS 7.1.2 Determination of Competence Criteria.....	3
7.2 Personnel involved in the certification activities.....	6
7.2.1 IS 7.2 Demonstration of auditor knowledge and experience.....	6
7.3 Use of individual external auditors and external technical experts.....	7
7.3.1 IS 7.3 Using external auditors or external technical experts as part of the audit team.....	7
7.4 Personnel records.....	7
7.5 Outsourcing.....	7
<b>8 Information requirements</b> .....	<b>8</b>
8.1 Public information.....	8
8.2 Certification documents.....	8
8.2.1 IS 8.2 ISMS Certification documents.....	8
8.3 Reference to certification and use of marks.....	8
8.4 Confidentiality.....	8
8.4.1 IS 8.4 Access to organizational records.....	8
8.5 Information exchange between a certification body and its clients.....	8
<b>9 Process requirements</b> .....	<b>8</b>
9.1 Pre-certification activities.....	8
9.1.1 Application.....	8
9.1.2 Application review.....	9
9.1.3 Audit programme.....	9
9.1.4 Determining audit time.....	10
9.1.5 Multi-site sampling.....	10
9.1.6 Multiple management systems.....	11
9.2 Planning audits.....	11
9.2.1 Determining audit objectives, scope and criteria.....	11
9.2.2 Audit team selection and assignments.....	12
9.2.3 Audit plan.....	12
9.3 Initial certification.....	13
9.3.1 IS 9.3.1 Initial certification audit.....	13
9.4 Conducting audits.....	14
9.4.1 IS 9.4 General.....	14
9.4.2 IS 9.4 Specific elements of the ISMS audit.....	14
9.4.3 IS 9.4 Audit report.....	14
9.5 Certification decision.....	15
9.5.1 IS 9.5 Certification decision.....	15

## ISO/IEC 27006:2015(E)

9.6	Maintaining certification .....	15
9.6.1	General .....	15
9.6.2	Surveillance activities .....	15
9.6.3	Re-certification .....	16
9.6.4	Special audits .....	17
9.6.5	Suspending, withdrawing or reducing the scope of certification .....	17
9.7	Appeals .....	17
9.8	Complaints .....	17
9.8.1	IS 9.8 Complaints .....	17
9.9	Client records .....	17
<b>10</b>	<b>Management system requirements for certification bodies .....</b>	<b>17</b>
10.1	Options .....	17
10.1.1	IS 10.1 ISMS implementation .....	17
10.2	Option A: General management system requirements .....	17
10.3	Option B: Management system requirements in accordance with ISO 9001 .....	17
<b>Annex A (informative) Knowledge and skills for ISMS auditing and certification .....</b>		<b>18</b>
<b>Annex B (normative) Audit time .....</b>		<b>20</b>
<b>Annex C (informative) Methods for audit time calculations .....</b>		<b>25</b>
<b>Annex D (informative) Guidance for review of implemented ISO/IEC 27001:2013, Annex A controls .....</b>		<b>28</b>
<b>Bibliography .....</b>		<b>35</b>

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

SIST EN ISO/IEC 27006:2021

<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021>

## 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](http://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](http://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.

**ISO/IEC 27006:2015(E)****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.

**iTeh STANDARD PREVIEW**  
**(standards.iteh.ai)**

[SIST EN ISO/IEC 27006:2021](https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021)

<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-907e78772c1f/sist-en-iso-iec-27006-2021>

# 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.

<https://standards.iteh.ai/catalog/standards/sist/ce0b0349-8c1d-4353-a187-c78772c1131c/sist-en-iso-iec-27006-2021>  
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.

## ISO/IEC 27006:2015(E)

### 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.