



SLOVENSKI STANDARD
SIST-TS CEN ISO/IEC/TS 27006-2:2023

01-januar-2023

Zahteve za organe, ki izvajajo presojanje in certificiranje sistemov upravljanja informacijske varnosti - 2. del: Sistemi za upravljanje informacij o zasebnosti (ISO/IEC/TS 27006-2:2021)

Requirements for bodies providing audit and certification of information security management systems - Part 2: Privacy information management systems (ISO/IEC/TS 27006-2:2021)

STANDARD PREVIEW
(standards.iteh.ai)

Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management des informations de sécurité - Partie 2: Systèmes de management des informations de sécurité (ISO/IEC/TS 27006-2:2021)

Ta slovenski standard je istoveten z: CEN ISO/IEC/TS 27006-2:2022

ICS:

03.120.20	Certificiranje proizvodov in podjetij. Ugotavljanje skladnosti	Product and company certification. Conformity assessment
35.030	Informacijska varnost	IT Security

SIST-TS CEN ISO/IEC/TS 27006-2:2023 en,fr,de

TECHNICAL SPECIFICATION

CEN ISO/IEC/TS 27006-2

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

November 2022

ICS 35.030; 03.120.20

English version

Requirements for bodies providing audit and certification
of information security management systems - Part 2:
Privacy information management systems (ISO/IEC TS
27006-2:2021)

Exigences pour les organismes procédant à l'audit et à
la certification des systèmes de management des
informations de sécurité - Partie 2: Systèmes de
management des informations de sécurité (ISO/IEC TS
27006-2:2021)

Anforderungen an Stellen, die Informationssicherheits-
Managementsysteme auditieren und zertifizieren - Teil
2: Datenschutz-Managementsysteme (ISO/IEC TS
27006-2:2021)

This Technical Specification (CEN/TS) was approved by CEN on 30 October 2022 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN and CENELEC will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN and CENELEC members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

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

Contents	Page
European foreword.....	3

iTeh STANDARD PREVIEW
(standards.iteh.ai)

SIST-TS CEN ISO/IEC/TS 27006-2:2023

<https://standards.iteh.ai/catalog/standards/sist/fb80be03-a69b-4777-a97c-5d0e3cc72d16/sist-ts-cen-iso-iec-ts-27006-2-2023>

European foreword

The text of ISO/IEC TS 27006-2:2021 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 CEN ISO/IEC/TS 27006-2:2022 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

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. 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 announce this Technical Specification: 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 TS 27006-2:2021 has been approved by CEN-CENELEC as CEN ISO/IEC/TS 27006-2:2022 without any modification.

[SIST-TS CEN ISO/IEC/TS 27006-2:2023](https://standards.iteh.ai/catalog/standards/sist/fb80be03-a69b-4777-a97c-5d0e3cc72d16/sist-ts-cen-iso-iec-ts-27006-2-2023)

<https://standards.iteh.ai/catalog/standards/sist/fb80be03-a69b-4777-a97c-5d0e3cc72d16/sist-ts-cen-iso-iec-ts-27006-2-2023>

TECHNICAL
SPECIFICATION

ISO/IEC TS
27006-2

First edition
2021-02

**Requirements for bodies providing
audit and certification of information
security management systems —**

**Part 2:
Privacy information management
systems**

*Exigences pour les organismes procédant à l'audit et à la certification
des systèmes de management des informations de sécurité —*

Partie 2: Systèmes de management des informations de sécurité

[SIST-TS CEN ISO/IEC/TS 27006-2:2023](https://standards.iteh.ai/catalog/standards/sist/fb80be03-a69b-4777-a97c-5d0e3cc72d16/sist-ts-cen-iso-iec-ts-27006-2-2023)

<https://standards.iteh.ai/catalog/standards/sist/fb80be03-a69b-4777-a97c-5d0e3cc72d16/sist-ts-cen-iso-iec-ts-27006-2-2023>



Reference number
ISO/IEC TS 27006-2:2021(E)

© ISO/IEC 2021

iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST-TS CEN ISO/IEC/TS 27006-2:2023

<https://standards.iteh.ai/catalog/standards/sist/fb80be03-a69b-4777-a97c-5d0e3cc72d16/sist-ts-cen-iso-iec-ts-27006-2-2023>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2021

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

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Principles	2
5 General requirements	2
5.1 Legal and contractual matters.....	2
5.2 Management of impartiality.....	2
5.3 Liability and financing.....	2
6 Structural requirements	2
7 Resource requirements	2
7.1 Competence of personnel.....	2
7.1.1 PS 7.1.1 General considerations.....	2
7.1.2 PS 7.1.2 Determination of competence criteria.....	2
7.2 Personnel involved in the certification activities.....	3
7.2.1 PS 7.2 Demonstration of auditor knowledge and experience.....	4
7.2.2 PS 7.2.1.1 Selecting auditors.....	4
7.3 Use of individual external auditors and external technical experts.....	4
7.4 Personnel records.....	4
7.5 Outsourcing.....	4
8 Information requirements	4
8.1 Public information.....	4
8.2 Certification documents.....	4
8.2.1 PS 8.2 PIMS Certification documents.....	4
8.3 Reference to certification and use of marks.....	5
8.4 Confidentiality.....	5
8.5 Information exchange between a certification body and its clients.....	5
9 Process requirements	5
9.1 Pre-certification activities.....	5
9.1.1 Application.....	5
9.1.2 Application review.....	5
9.1.3 Audit programme.....	5
9.1.4 Determining audit time.....	6
9.1.5 Multi-site sampling.....	7
9.1.6 Multiple management systems.....	7
9.2 Planning audits.....	7
9.2.1 Determining audit objectives, scope and criteria.....	7
9.2.2 Audit team selection and assignments.....	7
9.2.3 Audit plan.....	7
9.3 Initial certification.....	7
9.4 Conducting audits.....	7
9.4.1 IS 9.4 General.....	7
9.4.2 IS 9.4 Specific elements of the ISMS audit.....	7
9.4.3 IS 9.4 Audit report.....	7
9.5 Certification decision.....	7
9.6 Maintaining certification.....	8
9.6.1 General.....	8
9.6.2 Surveillance activities.....	8
9.6.3 Re-certification.....	8
9.6.4 Special audits.....	8

ISO/IEC TS 27006-2:2021(E)

	9.6.5	Suspending, withdrawing or reducing the scope of certification.....	8
9.7		Appeals.....	8
9.8		Complaints.....	8
9.9		Client records.....	8
10		Management system requirements for certification bodies	8
10.1		Options.....	8
10.2		Option A: General management system requirements.....	8
10.3		Option B: Management system requirements in accordance with ISO 9001.....	9

iTeh STANDARD PREVIEW

(standards.itih.ai)

[SIST-TS CEN ISO/IEC/TS 27006-2:2023](https://standards.itih.ai/catalog/standards/sist/fb80be03-a69b-4777-a97c-5d0e3cc72d16/sist-ts-cen-iso-iec-ts-27006-2-2023)

<https://standards.itih.ai/catalog/standards/sist/fb80be03-a69b-4777-a97c-5d0e3cc72d16/sist-ts-cen-iso-iec-ts-27006-2-2023>

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).

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) or the IEC list of patent declarations received (see patents.iec.ch).

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.

This document was prepared by Joint Technical Committee ISO/JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 27006 series can be found on the ISO website.

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.