



BSI Standards Publication

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

Part 2: Privacy information management systems

National foreword

This Published Document is the UK implementation of CEN ISO/IEC/TS 27006-2:2022. It is identical to ISO/IEC TS 27006-2:2021. It supersedes PD ISO/IEC TS 27006-2:2021, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/35, Health informatics.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 22030 8

ICS 03.120.20; 35.030

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 31 March 2021.

Amendments/corrigenda issued since publication

Date	Text affected
30 April 2023	This corrigendum renumbers PD ISO/IEC TS 27006-2:2021 as PD CEN ISO/IEC/TS 27006-2:2022

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

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.

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

	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