

Tecnología de la información. Técnicas de seguridad. Requisitos para organismos que realizan auditorías y certificación de sistemas de gestión de seguridad de la información (ISO/IEC 27006:2015, incluyendo Amd 1:2020) (Ratificada por la Asociación Española de Normalización en enero de 2021.)

UNE-EN ISO/IEC 27006:2020

Tecnología de la información. Técnicas de seguridad. Requisitos para organismos que realizan auditorías y certificación de sistemas de gestión de seguridad de la información (ISO/IEC 27006:2015, incluyendo Amd 1:2020) (Ratificada por la Asociación Española de Normalización en enero de 2021.)

Information technology - Security techniques - Requirements for bodies providing audit and certification of information security management systems (ISO/IEC 27006:2015, including Amd 1:2020) (Endorsed by Asociación Española de Normalización in January of 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) (Entérinée par l'Asociación Española de Normalización en janvier 2021.)

En cumplimiento del punto 11.2.5.4 de las Reglas Internas de CEN/CENELEC Parte 2, se ha otorgado el rango de documento normativo español UNE al documento normativo europeo EN ISO/IEC 27006:2020 (Fecha de disponibilidad 2020-11-25)

Este documento está disponible en los idiomas oficiales de CEN/CENELEC/ETSI.

Este anuncio causará efecto a partir del primer día del mes siguiente al de su publicación en la revista UNE.

La correspondiente versión oficial de este documento se encuentra disponible en la Asociación Española de Normalización (Génova 6 28004 MADRID, www.une.org).

Esta versión corregida de la Norma UNE-EN ISO/IEC 27006:2020 incorpora las siguientes correcciones:
Se adjunta nueva versión en inglés de la Norma EN ISO/IEC 27006:2020.

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización

Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

© UNE 2021

Prohibida la reproducción sin el consentimiento de UNE.

Todos los derechos de propiedad intelectual de la presente norma son titularidad de UNE.

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)

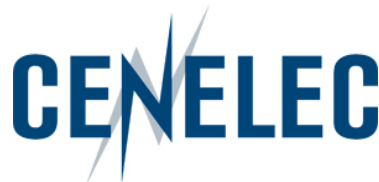
This European Standard was approved by CEN on 16 November 2020.

This European Standard was corrected and reissued by the CEN-CENELEC Management Centre on 24 February 2021.

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.



Contents	Page
European foreword.....	3

European foreword

The text of ISO/IEC 27006:2015, including Amd 1:2020, 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.

Endorsement notice

The text of ISO/IEC 27006:2015, including Amd 1:2020, has been approved by CEN as EN ISO/IEC 27006:2020 without any modification.

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Principles	1
5 General requirements	2
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
6 Structural requirements	2
7 Resource requirements	2
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
8 Information requirements	8
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
9 Process requirements	8
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

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
10	Management system requirements for certification bodies	17
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
	Annex A (informative) Knowledge and skills for ISMS auditing and certification	18
	Annex B (normative) Audit time	20
	Annex C (informative) Methods for audit time calculations	25
	Annex D (informative) Guidance for review of implemented ISO/IEC 27001:2013,	
	Annex A controls	28
	Bibliography	35