

ILNAS

Institut luxembourgeois de la normalisation
de l'accréditation, de la sécurité et qualité
des produits et services

ILNAS-EN 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

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

Cybersicherheit und Datenschutz -
Anforderungen an Stellen, die
Informationssicherheitsmanagementsyst
eme auditieren und zertifizieren - Teil 1:

03/2024



Avant-propos national

Cette Norme Européenne EN ISO/IEC 27006-1:2024 a été adoptée comme Norme Luxembourgeoise ILNAS-EN ISO/IEC 27006-1:2024.

Toute personne intéressée, membre d'une organisation basée au Luxembourg, peut participer gratuitement à l'élaboration de normes luxembourgeoises (ILNAS), européennes (CEN, CENELEC) et internationales (ISO, IEC) :

- Influencer et participer à la conception de normes
- Anticiper les développements futurs
- Participer aux réunions des comités techniques

<https://portail-qualite.public.lu/fr/normes-normalisation/participer-normalisation.html>

CETTE PUBLICATION EST PROTÉGÉE PAR LE DROIT D'AUTEUR

Aucun contenu de la présente publication ne peut être reproduit ou utilisé sous quelque forme ou par quelque procédé que ce soit - électronique, mécanique, photocopie ou par d'autres moyens sans autorisation préalable !

ILNAS-EN ISO/IEC 27006-1:2024
NORME EUROPÉENNE **EN ISO/IEC 27006-1**
EUROPÄISCHE NORM
EUROPEAN STANDARD
Mars 2024

ICS 03.120.20; 35.030

Remplace l' EN ISO/IEC 27006:2020

Version Française

**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
Informationssicherheitsmanagementsysteme
auditieren und zertifizieren - Teil 1: Allgemeines
(ISO/IEC 27006-1:2024)

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)

La présente Norme européenne a été adoptée par le CEN le 29 janvier 2024.

Cette norme européenne a été corrigée et rééditée par le Centre de gestion du CEN-CENELEC le 20 Mars 2024.

Les membres du CEN et CENELEC sont tenus de se soumettre au Règlement Intérieur du CEN/CENELEC, qui définit les conditions dans lesquelles doit être attribué, sans modification, le statut de norme nationale à la Norme européenne. Les listes mises à jour et les références bibliographiques relatives à ces normes nationales peuvent être obtenues auprès du Centre de Gestion du CEN-CENELEC ou auprès des membres du CEN et CENELEC.

La présente Norme européenne existe en trois versions officielles (allemand, anglais, français). Une version dans une autre langue faite par traduction sous la responsabilité d'un membre du CEN et CENELEC dans sa langue nationale et notifiée au Centre de Gestion du CEN-CENELEC, a le même statut que les versions officielles.

Les membres du CEN et du CENELEC sont les organismes nationaux de normalisation et les comités électrotechniques nationaux des pays suivants: Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République de Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.



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

Sommaire

Page

Avant-propos européen	3
-----------------------------	---

Avant-propos européen

Le présent document (EN ISO/IEC 27006-1:2024) a été élaboré par le Comité Technique ISO/IEC JTC 1 « Technologies de l'information » en collaboration avec le Comité Technique CEN-CENELEC/ JTC 13 « Cybersécurité et protection des données » dont le secrétariat est tenu par DIN.

La présente Norme européenne devra recevoir le statut de norme nationale, soit par publication d'un texte identique, soit par entérinement, au plus tard en septembre 2024 et les normes nationales en contradiction devront être retirées au plus tard en septembre 2024.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. Le CEN et/ou le CENELEC ne sauraient être tenus pour responsables de l'identification de ces droits de propriété en tout ou partie.

Ce document remplace l'EN ISO/IEC 27006:2020.

Il convient que l'utilisateur adresse tout retour d'information et toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve sur les sites web du CEN et du CENELEC.

Selon le règlement intérieur du CEN/CENELEC, les instituts de normalisation nationaux des pays suivants sont tenus de mettre cette Norme européenne en application : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Islande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République de Macédoine du Nord, République tchèque, Roumanie, Royaume-Uni, Serbie, Slovaquie, Slovénie, Suède, Suisse et Turquie.

Notice d'entérinement

Le texte de l'ISO/IEC 27006-1:2024 a été approuvé par le CEN-CENELEC en tant que EN ISO/IEC 27006-1:2024 sans aucune modification.



ILNAS-EN ISO/IEC 27006-1:2024

Norme internationale

ISO/IEC 27006-1

Première édition
2024-03

ILNAS-FIN ISO/IEC 27006-1:2024 - Preview only Copy via ILNAS e-Shop

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

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

Part 1: General



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2024

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos	v
Introduction	vii
1 Domaine d'application	1
2 Références normatives	1
3 Termes et définitions	1
4 Principes	5
5 Exigences générales	5
5.1 Domaine juridique et contractuel	5
5.2 Gestion de l'impartialité	5
5.2.1 Généralités	5
5.2.2 Conflits d'intérêts	5
5.3 Responsabilité et situation financière	5
6 Exigences structurelles	5
7 Exigences relatives aux ressources	5
7.1 Compétence du personnel	5
7.1.1 Généralités	5
7.1.2 Exigences génériques en matière de compétence	6
7.1.3 Détermination des critères de compétence	6
7.2 Personnel intervenant dans les activités de certification	9
7.2.1 Généralités	9
7.2.2 Démonstration des connaissances et de l'expérience des auditeurs	9
7.3 Intervention d'auditeurs et d'experts techniques externes individuels	10
7.4 Enregistrements relatifs au personnel	10
7.5 Externalisation	10
8 Exigences relatives aux informations	10
8.1 Informations publiques	10
8.2 Documents de certification	10
8.2.1 Généralités	10
8.2.2 Documents de certification SMSI	10
8.2.3 Référence à d'autres normes dans les documents de certification SMSI	10
8.3 Référence à la certification et utilisation des marques	11
8.4 Confidentialité	11
8.4.1 Généralités	11
8.4.2 Accès aux enregistrements de l'organisation	11
8.5 Échange d'informations entre l'organisme de certification et ses clients	11
9 Exigences relatives aux processus	11
9.1 Activités préalables à la certification	11
9.1.1 Demande de certification	11
9.1.2 Revue de la demande	12
9.1.3 Programme d'audit	12
9.1.4 Détermination du temps d'audit	13
9.1.5 Échantillonnage multisite	13
9.1.6 Systèmes de management multiples	15
9.2 Planification des audits	15
9.2.1 Détermination des objectifs, du domaine d'application et des critères de l'audit	15
9.2.2 Constitution de l'équipe d'audit et affectation des missions	15
9.2.3 Plan d'audit	16
9.3 Certification initiale	16
9.3.1 Généralités	16
9.3.2 Audit de certification initiale	16
9.4 Réalisation des audits	17