

# ILNAS

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

## ILNAS-EN ISO/IEC 27006:2020

### **Technologies de l'information - Techniques de sécurité - Exigences pour les organismes procédant à l'audit et à la certification des**

Information technology - Security  
techniques - Requirements for bodies  
providing audit and certification of  
information security management

Informationstechnik - IT-  
Sicherheitsverfahren - Anforderungen an  
Institutionen, die Audits und  
Zertifizierungen von

11/2020



## Avant-propos national

Cette Norme Européenne EN ISO/IEC 27006:2020 a été adoptée comme Norme Luxembourgeoise ILNAS-EN ISO/IEC 27006:2020.

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 !

Version Française

**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)

Information technology - Security techniques -  
Requirements for bodies providing audit and  
certification of information security management  
systems (ISO/IEC 27006:2015, including Amd 1:2020)

La présente Norme européenne a été adoptée par le CEN le 16 novembre 2020.

Cette norme européenne a été corrigée et rééditée par le Centre de gestion du CEN-CENELEC le 24 février 2021.

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**

ILNAS-EN ISO/IEC 27006:2020 - Preview only Copy via ILNAS e-Shop

## Avant-propos européen

Le texte de l'ISO/IEC 27006:2015, y compris Amd 1:2020, a été élaboré par le Comité technique ISO/IEC JTC 1 « Technologies de l'information » de l'Organisation internationale de normalisation (ISO) et a été repris comme EN ISO/IEC 27006:2020 par le Comité technique CEN/CLC/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 mai 2021 et les normes nationales en contradiction devront être retirées au plus tard en mai 2021.

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 ne saurait être tenu responsable de l'identification de tels ou tels brevets.

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 27006:2015, y compris Amd 1:2020, a été approuvé par le CEN comme EN ISO/IEC 27006:2020 sans aucune modification.

---

---

**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**

*Information technology — Security techniques — Requirements  
for bodies providing audit and certification of information security  
management systems*



**DOCUMENT PROTÉGÉ PAR COPYRIGHT**

© ISO/IEC 2015

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](mailto:copyright@iso.org)

Web: [www.iso.org](http://www.iso.org)

Publié en Suisse

# Sommaire

Page

<b>Avant-propos</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Domaine d'application</b> .....	<b>1</b>
<b>2 Références normatives</b> .....	<b>1</b>
<b>3 Termes et définitions</b> .....	<b>1</b>
<b>4 Principes</b> .....	<b>1</b>
<b>5 Exigences générales</b> .....	<b>2</b>
5.1 Domaine juridique et contractuel.....	2
5.2 Gestion de l'impartialité.....	2
5.2.1 SI 5.2 Conflits d'intérêts.....	2
5.3 Responsabilité et situation financière.....	2
<b>6 Exigences structurelles</b> .....	<b>2</b>
<b>7 Exigences relatives aux ressources</b> .....	<b>2</b>
7.1 Compétence du personnel.....	2
7.1.1 SI 7.1.1 Considérations générales.....	3
7.1.2 SI 7.1.2 Détermination des critères de compétence.....	3
7.2 Personnel intervenant dans les activités de certification.....	7
7.2.1 SI 7.2 Démonstration des connaissances et de l'expérience des auditeurs.....	7
7.3 Intervention d'auditeurs et d'experts techniques externes individuels.....	8
7.3.1 SI 7.3 Intervention d'auditeurs externes ou d'experts techniques externes au sein de l'équipe d'audit.....	8
7.4 Enregistrements relatifs au personnel.....	8
7.5 Externalisation.....	8
<b>8 Exigences relatives aux informations</b> .....	<b>8</b>
8.1 Informations publiques.....	8
8.2 Documents de certification.....	8
8.2.1 SI 8.2 Documents de certification SMSI.....	8
8.3 Référence à la certification et utilisation des marques.....	9
8.4 Confidentialité.....	9
8.4.1 SI 8.4 Accès aux enregistrements de l'organisation.....	9
8.5 Échange d'informations entre l'organisme de certification et ses clients.....	9
<b>9 Exigences relatives aux processus</b> .....	<b>9</b>
9.1 Activités préalables à la certification.....	9
9.1.1 Demande de certification.....	9
9.1.2 Revue de la demande.....	9
9.1.3 Programme d'audit.....	9
9.1.4 Détermination du temps d'audit.....	10
9.1.5 Échantillonnage multisite.....	11
9.1.6 Systèmes de management multiples.....	12
9.2 Planification des audits.....	12
9.2.1 Détermination des objectifs, du domaine d'application et des critères de l'audit.....	12
9.2.2 Constitution de l'équipe d'audit et affectation des missions.....	12
9.2.3 Plan d'audit.....	13
9.3 Certification initiale.....	14
9.3.1 SI 9.3.1 Audit de certification initiale.....	14
9.4 Réalisation des audits.....	15
9.4.1 SI 9.4 Généralités.....	15
9.4.2 SI 9.4 Éléments spécifiques de l'audit de SMSI.....	15
9.4.3 SI 9.4 Rapport d'audit.....	15
9.5 Décision de certification.....	16