

ILNAS

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

ILNAS-EN ISO/IEC 27001:2023

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences

Information security, cybersecurity and
privacy protection - Information security
management systems - Requirements
(ISO/IEC 27001:2022)

Informationssicherheit, Cybersicherheit
und Datenschutz -
Informationssicherheitsmanagementsyst
eme - Anforderungen (ISO/IEC

07/2023



Avant-propos national

Cette Norme Européenne EN ISO/IEC 27001:2023 a été adoptée comme Norme Luxembourgeoise ILNAS-EN ISO/IEC 27001:2023.

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

Sécurité de l'information, cybersécurité et protection de la vie privée - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2022)

Informationssicherheit, Cybersicherheit und
Datenschutz -
Informationssicherheitsmanagementsysteme -
Anforderungen (ISO/IEC 27001:2022)

Information security, cybersecurity and privacy
protection - Information security management systems
- Requirements (ISO/IEC 27001:2022)

La présente Norme européenne a été adoptée par le CEN le 23 juillet 2023.

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 27001:2023 - Preview only Copy via ILNAS e-Shop

Avant-propos européen

Le texte de l'ISO/IEC 27001:2022 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 27001:2023 par 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 janvier 2024 et les normes nationales en contradiction devront être retirées au plus tard en janvier 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 27001:2017.

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 27001:2022 a été approuvé par le CEN-CENELEC comme EN ISO/IEC 27001:2023 sans aucune modification.

**Sécurité de l'information,
cybersécurité et protection de la vie
privée — Systèmes de management
de la sécurité de l'information —
Exigences**

*Information security, cybersecurity and privacy protection —
Information security management systems — Requirements*

**DOCUMENT PROTÉGÉ PAR COPYRIGHT**

© ISO/IEC 2022

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
Fax: +41 22 749 09 47
E-mail: copyright@iso.org
Web: www.iso.org

Publié en Suisse

Sommaire

Page

| | |
|--|-----------|
| Avant-propos | iv |
| Introduction | v |
| 1 Domaine d'application | 1 |
| 2 Références normatives | 1 |
| 3 Termes et définitions | 1 |
| 4 Contexte de l'organisation | 1 |
| 4.1 Compréhension de l'organisation et de son contexte | 1 |
| 4.2 Compréhension des besoins et attentes des parties intéressées | 2 |
| 4.3 Détermination du domaine d'application du système de management de la sécurité de l'information | 2 |
| 4.4 Système de management de la sécurité de l'information | 2 |
| 5 Leadership | 2 |
| 5.1 Leadership et engagement | 2 |
| 5.2 Politique | 3 |
| 5.3 Rôles, responsabilités et autorités au sein de l'organisation | 3 |
| 6 Planification | 3 |
| 6.1 Actions à mettre en œuvre face aux risques et opportunités | 3 |
| 6.1.1 Généralités | 3 |
| 6.1.2 Appréciation des risques de sécurité de l'information | 4 |
| 6.1.3 Traitement des risques de sécurité de l'information | 5 |
| 6.2 Objectifs de sécurité de l'information et plans pour les atteindre | 5 |
| 6.3 Planification des modifications | 6 |
| 7 Supports | 6 |
| 7.1 Ressources | 6 |
| 7.2 Compétences | 6 |
| 7.3 Sensibilisation | 6 |
| 7.4 Communication | 7 |
| 7.5 Informations documentées | 7 |
| 7.5.1 Généralités | 7 |
| 7.5.2 Création et mise à jour | 7 |
| 7.5.3 Contrôle des informations documentées | 7 |
| 8 Fonctionnement | 8 |
| 8.1 Planification et contrôle opérationnels | 8 |
| 8.2 Appréciation des risques de sécurité de l'information | 8 |
| 8.3 Traitement des risques de sécurité de l'information | 8 |
| 9 Évaluation de la performance | 8 |
| 9.1 Surveillance, mesurages, analyse et évaluation | 8 |
| 9.2 Audit interne | 9 |
| 9.2.1 Généralités | 9 |
| 9.2.2 Programme d'audit interne | 9 |
| 9.3 Revue de direction | 9 |
| 9.3.1 Généralités | 9 |
| 9.3.2 Éléments d'entrée de la revue de direction | 9 |
| 9.3.3 Résultats des revues de direction | 10 |
| 10 Amélioration | 10 |
| 10.1 Amélioration continue | 10 |
| 10.2 Non-conformité et action corrective | 10 |
| Annexe A (normative) Référencement des mesures de sécurité de l'information | 12 |
| Bibliographie | 21 |