

ILNAS

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

ILNAS-EN ISO/IEC 27001:2017

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC

Informationstechnik -
Sicherheitsverfahren -
Informationssicherheitsmanagementsyst
eme - Anforderungen (ISO/IEC

Information technology - Security
techniques - Information security
management systems - Requirements
(ISO/IEC 27001:2013 including Cor 1:2014

02/2017



Avant-propos national

Cette Norme Européenne EN ISO/IEC 27001:2017 a été adoptée comme Norme Luxembourgeoise ILNAS-EN ISO/IEC 27001:2017.

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 27001:2017

NORME EUROPÉENNE **EN ISO/IEC 27001**

EUROPÄISCHE NORM

EUROPEAN STANDARD

Février 2017

ICS 03.100.70; 35.030

Version Française

**Technologies de l'information - Techniques de sécurité -
Systèmes de management de la sécurité de l'information -
Exigences (ISO/IEC 27001:2013 y compris Cor 1:2014 et
Cor 2:2015)**

Informationstechnik - Sicherheitsverfahren -
Informationssicherheits-Managementsysteme -
Anforderungen (ISO/IEC 27001:2013 einschließlich
Cor 1:2014 und Cor 2:2015)

Information technology - Security techniques -
Information security management systems -
Requirements (ISO/IEC 27001:2013 including Cor
1:2014 and Cor 2:2015)

La présente Norme européenne a été adoptée par le CEN le 26 janvier 2017.

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, Ancienne République yougoslave de Macédoine, 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 Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.



COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION

CEN-CENELEC Management Centre: Avenue Marnix 17, B-1000 Bruxelles

Sommaire

Page

Avant-propos européen 3

ILNAS-EN ISO/IEC 27001:2017 - Preview only Copy via ILNAS e-Shop

Avant-propos européen

Le texte de l'ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015 a été élaboré par le Comité Technique ISO/CEI JTC 1 "Technologies de l'information" de l'Organisation Internationale de Normalisation (ISO) et la Commission Internationale Electrotechnique (CEI) et a été repris comme EN ISO/IEC 27001:2017.

Cette Norme européenne devra recevoir le statut de norme nationale, soit par publication d'un texte identique, soit par entérinement, au plus tard en août 2017, et toutes les normes nationales en contradiction devront être retirées au plus tard en août 2017.

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 saurait [sauraient] être tenu[s] pour responsable[s] de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

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, Ancienne République Yougoslave de Macédoine, 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 Serbie, République Tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse et Turquie.

Notice d'entérinement

Le texte de ISO/IEC 27001:2013 y compris Cor 1:2014 et Cor 2:2015 a été approuvé par le CEN comme EN ISO/IEC 27001:2017 sans aucune modification.

**Technologies de l'information —
Techniques de sécurité — Systèmes
de management de la sécurité de
l'information — Exigences**

*Information technology — Security techniques — Information
security management systems — Requirements*

**DOCUMENT PROTÉGÉ PAR COPYRIGHT**

© ISO/CEI 2013

Droits de reproduction réservés. Sauf indication contraire, 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, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées 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 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Version française parue en 2013

Publié en Suisse

Sommaire

Page

Avant-propos	iv
0 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 des attentes des parties intéressées.....	1
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.....	2
5.3 Rôles, responsabilités et autorités au sein de l'organisation.....	3
6 Planification	3
6.1 Actions liées aux risques et opportunités.....	3
6.2 Objectifs de sécurité de l'information et plans pour les atteindre.....	5
7 Support	5
7.1 Ressources.....	5
7.2 Compétence.....	6
7.3 Sensibilisation.....	6
7.4 Communication.....	6
7.5 Informations documentées.....	6
8 Fonctionnement	7
8.1 Planification et contrôle opérationnels.....	7
8.2 Appréciation des risques de sécurité de l'information.....	8
8.3 Traitement des risques de sécurité de l'information.....	8
9 Évaluation des performances	8
9.1 Surveillance, mesures, analyse et évaluation.....	8
9.2 Audit interne.....	8
9.3 Revue de direction.....	9
10 Amélioration	9
10.1 Non-conformité et actions correctives.....	9
10.2 Amélioration continue.....	10
Annexe A (normative) Objectifs et mesures de référence	11
Bibliographie	23