Norme Belge

ISO/IEC 27001:2022

NBN 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 (ISO/IEC 27001:2022)

Valable à partir de 16-01-2023

Cette norme ne remplace pas la NBN EN ISO/IEC 27001:2017, cette version sera retirée une fois la version européenne adoptée. Le NBN, en tant que membre du CEN, est normalement tenu d’attendre la publication de la version européenne (obligation de statu quo). Le CEN/CENELEC a convenu d'accorder une dérogation au ‘statu quo’ à tous les membres du CEN et du CENELEC pour l'ISO/IEC 27001:2022.

ICS: 03.100.70; 35.030

Bureau de Normalisation
Rue Joseph-II 40 bte 6
1000 Bruxelles

T. +32 2 738 01 11
F. +32 2 733 42 64
production@nbn.be

TVA BE0880.857.592
IBAN BE41 0003 2556 2110
BIC Code BPOTBEB1

www.nbn.be

Avant- propos national

Cette norme a été élaborée par ISO/IEC JTC 1, Technologies de l'information, SC 27, Sécurité de l'information, cybersécurité et protection de la vie privée.

Cette norme est publiée comme norme belge par le NBN sans aucune modification.

Cette norme ne remplace pas la NBN EN ISO/IEC 27001:2017, cette version sera retirée une fois la version européenne adoptée.

Le NBN, en tant que membre du CEN, est normalement tenu d'attendre la publication de la version européenne (obligation de statu quo).

Le CEN/CENELEC a convenu d'accorder une dérogation au 'statu quo' à tous les membres du CEN et du CENELEC pour l'ISO/IEC 27001:2022.

Nationaal voorwoord

Deze norm is opgesteld door ISO/IEC JTC 1, Information technology, SC 27, Information security, cybersecurity and privacy protection.

Deze norm werd door het NBN ongewijzigd gepubliceerd als Belgische norm.

Deze norm vervangt NBN EN ISO/IEC 27001:2017 niet, deze versie zal worden ingetrokken zodra de Europese versie is goedgekeurd.

Het NBN is als lid van CEN normaliter verplicht te wachten op de publicatie van de Europese versie (standstill-verplichting).

CEN/CENELEC stemde ermee in om aan alle CEN- en CENELEC-leden een afwijking van 'standstill' te verlenen voor ISO/IEC 27001:2022.

NBN ISO/IEC 27001:2023

NORME INTERNATIONALE

ISO/IEC 27001

Troisième édition
2022-10

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

Numéro de référence
ISO/IEC 27001:2022(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

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

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et l'IEC, participent également aux travaux.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ~~ISO~~. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives ou www.iec.ch/members_experts/refdocs).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets) ou dans la liste des déclarations de brevets reçues par l'IEC (voir https://patents.iec.ch).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir www.iso.org/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27001:2013) qui a fait l'objet d'une révision technique. Elle incorpore également les Rectificatifs techniques ISO/IEC 27001:2013/Cor 1:2014 et ISO/IEC 27001:2013/Cor 2:2015.

Les principales modifications sont les suivantes :

— le texte a été aligné avec la structure harmonisée des normes de système de management et l'ISO/IEC 27002:2022.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/members.html et www.iec.ch/national-committees.

Introduction

0.1 Généralités

Le présent document a été élaboré pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l'information. L'adoption d'un système de management de la sécurité de l'information relève d'une décision stratégique de l'organisation. L'établissement et la mise en œuvre d'un système de management de la sécurité de l'information d'une organisation tiennent compte des besoins et des objectifs de l'organisation, des exigences de sécurité, des processus organisationnels mis en œuvre, ainsi que de la taille et de la structure de l'organisation. Tous ces facteurs d'influence sont appelés à évoluer dans le temps.

Le système de management de la sécurité de l'information préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate.

Il est important que le système de management de la sécurité de l'information fasse partie intégrante des processus et de la structure de management d'ensemble de l'organisation et que la sécurité de l'information soit prise en compte dans la conception des processus, des systèmes d'information et des mesures de sécurité. Il est prévu qu'un système de management de la sécurité de l'information évolue conformément aux besoins de l'organisation.

Le présent document peut être utilisé par les parties internes et externes pour évaluer la capacité de l'organisation à répondre à ses propres exigences en matière de sécurité de l'information.

L'ordre dans lequel les exigences sont présentées dans le présent document ne reflète pas leur importance ni l'ordre dans lequel elles doivent être mises en œuvre. Les éléments des listes sont énumérés uniquement à des fins de référence.

L'ISO/IEC 27000 décrit une vue d'ensemble et le vocabulaire des systèmes de management de la sécurité de l'information, en se référant à la famille des normes du système de management de la sécurité de l'information (incluant l'ISO/IEC 27003,[2] l'ISO/IEC 27004[3] et l'ISO/IEC 27005[4]) avec les termes et les définitions qui s'y rapportent.

0.2 Compatibilité avec d'autres systèmes de management

Le présent document applique la structure de haut niveau, les titres de paragraphe identiques, le texte, les termes communs et les définitions fondamentales définies dans l'Annexe SL des Directives ISO/IEC, Partie 1, Supplément ISO consolidé, et, par conséquent, est compatible avec les autres normes de systèmes de management qui se conforment à l'Annexe SL.

Cette approche commune définie dans l'Annexe SL sera utile aux organisations qui choisissent de mettre en œuvre un système de management unique pour répondre aux exigences de deux ou plusieurs normes de systèmes de management.