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)

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.

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

1 Domaine d'application

Le présent document spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. Le présent document comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation. Les exigences fixées dans le présent document sont génériques et prévues pour s'appliquer à toute organisation, quels que soient son type, sa taille et sa nature. Il n'est pas admis qu'une organisation s'affranchisse de l'une des exigences spécifiées aux Articles 4 à 10 lorsqu'elle revendique la conformité au présent document.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences du présent document. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

ISO/IEC 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO/IEC 27000 s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

4 Contexte de l'organisation

4.1 Compréhension de l'organisation et de son contexte

L'organisation doit déterminer les enjeux externes et internes pertinents compte tenu de sa mission et qui ont une incidence sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son système de management de la sécurité de l'information.

NOTE Déterminer ces enjeux revient à établir le contexte externe et interne de l'organisation étudiée dans le paragraphe 5.4.1 de l'ISO 31000:2018[5].

4.2 Compréhension des besoins et attentes des parties intéressées

L'organisation doit déterminer :

a) les parties intéressées qui sont concernées par le système de management de la sécurité de l'information ;

b) les exigences pertinentes de ces parties intéressées ;

c) lesquelles de ces exigences seront traitées par le biais du système de management de la sécurité de l'information.

NOTE Les exigences des parties intéressées peuvent inclure des exigences légales et réglementaires et des obligations contractuelles.

4.3 Détermination du domaine d'application du système de management de la sécurité de l'information

Pour établir le domaine d'application du système de management de la sécurité de l'information, l'organisation doit en déterminer les limites et l'applicabilité.

Lorsque l'organisation établit ce domaine d'application, elle doit prendre en compte :

a) les enjeux externes et internes auxquels il est fait référence en 4.1 ;

b) les exigences auxquelles il est fait référence en 4.2 ;

c) les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations.

Le domaine d'application doit être disponible sous la forme d'une information documentée.

4.4 Système de management de la sécurité de l'information

L'organisation doit établir, mettre en œuvre, tenir à jour et améliorer en continu un système de management de la sécurité de l'information, y compris les processus nécessaires et leurs interactions, en accord avec les exigences du présent document.

5 Leadership

5.1 Leadership et engagement

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management de la sécurité de l'information en :

a) s'assurant qu'une politique et des objectifs sont établis en matière de sécurité de l'information et qu'ils sont compatibles avec l'orientation stratégique de l'organisation ;

b) s'assurant que les exigences liées au système de management de la sécurité de l'information sont intégrées aux processus métiers de l'organisation ;

c) s'assurant que les ressources nécessaires pour le système de management de la sécurité de l'information sont disponibles ;

d) communiquant sur l'importance de disposer d'un management de la sécurité de l'information efficace et de se conformer aux exigences du système de management de la sécurité de l'information ;

e) s'assurant que le système de management de la sécurité de l'information produit le(s) résultat(s) escompté(s) ;

f) orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du système de management de la sécurité de l'information ;

g) promouvant l'amélioration continue ; et

h) aidant les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités.

NOTE Dans le présent document, il est possible d'interpréter le terme « métier » au sens large, c'est-à-dire comme se référant aux activités liées à la finalité de l'organisation.

5.2 Politique

La direction doit établir une politique de sécurité de l'information qui :

a) est appropriée à la mission de l'organisation ;

b) inclut des objectifs de sécurité de l'information (voir 6.2) ou fournit un cadre pour l'établissement de ces objectifs ;

c) inclut l'engagement de satisfaire aux exigences applicables en matière de sécurité de l'information ;

d) inclut l'engagement d'œuvrer pour l'amélioration continue du système de management de la sécurité de l'information.

La politique de sécurité de l'information doit :

e) être disponible sous forme d'information documentée ;

f) être communiquée au sein de l'organisation ;

g) être mise à la disposition des parties intéressées, le cas échéant.

5.3 Rôles, responsabilités et autorités au sein de l'organisation

La direction doit s'assurer que les responsabilités et autorités des rôles concernés par la sécurité de l'information sont attribuées et communiquées au sein de l'organisation.

La direction doit attribuer la responsabilité et l'autorité pour :

a) s'assurer que le système de management de la sécurité de l'information est conforme aux exigences du présent document ;

b) rendre compte à la direction des performances du système de management de la sécurité de l'information.

NOTE La direction peut également attribuer des responsabilités et autorités pour rendre compte des performances du système de management de la sécurité de l'information au sein de l'organisation.

6 Planification

6.1 Actions à mettre en œuvre face aux risques et opportunités

6.1.1 Généralités

Lorsqu'il conçoit son système de management de la sécurité de l'information, l'organisation doit tenir compte des enjeux de 4.1 et des exigences de 4.2, et déterminer les risques et opportunités qui nécessitent d'être abordés pour :

a) s'assurer que le système de management de la sécurité de l'information peut atteindre le(s) résultat(s) escompté(s) ;

b) empêcher ou limiter les effets indésirables ; et

c) obtenir une démarche d'amélioration continue.

L'organisation doit planifier :

d) les actions menées pour traiter ces risques et opportunités ; et

e) la manière :

1) d'intégrer et de mettre en œuvre les actions au sein des processus du système de management de la sécurité de l'information ; et

2) d'évaluer l'efficacité de ces actions.

6.1.2 Appréciation des risques de sécurité de l'information

L'organisation doit définir et appliquer un processus d'appréciation des risques de sécurité de l'information qui :

a) établit et tient à jour les critères de risque de sécurité de l'information incluant :

1) les critères d'acceptation des risques ;

2) les critères de réalisation des appréciations des risques de sécurité de l'information ;

b) s'assure que la répétition de ces appréciations des risques produit des résultats cohérents, valides et comparables ;

c) identifie les risques de sécurité de l'information :

1) applique le processus d'appréciation des risques de sécurité de l'information pour identifier les risques de perte de confidentialité, d'intégrité et de disponibilité des informations entrant dans le domaine d'application du système de management de la sécurité de l'information ; et

2) identifie les propriétaires des risques ;

d) analyse les risques de sécurité de l'information :

1) apprécie les conséquences potentielles dans le cas où les risques identifiés en 6.1.2 c) 1) se concrétisaient ;

2) procède à une évaluation réaliste de la vraisemblance d'apparition des risques identifiés en 6.1.2 c) 1) ; et

3) détermine les niveaux des risques ;

e) évalue les risques de sécurité de l'information :

1) compare les résultats d'analyse des risques avec les critères de risque déterminés en 6.1.2 a) ; et

2) priorise les risques analysés pour le traitement des risques.

L'organisation doit conserver des informations documentées sur le processus d'appréciation des risques de sécurité de l'information.

6.1.3 Traitement des risques de sécurité de l'information

L'organisation doit définir et appliquer un processus de traitement des risques de sécurité de l'information pour :

a) choisir les options de traitement des risques appropriées, en tenant compte des résultats de l'appréciation des risques ;

b) déterminer toutes les mesures de sécurité nécessaires à la mise en œuvre de(s) (l')option(s) de traitement des risques de sécurité de l'information choisie(s) ;

NOTE 1 Les organisations peuvent concevoir ces mesures de sécurité, le cas échéant, ou bien les identifier à partir de n'importe quelle source.

c) comparer les mesures de sécurité déterminées ci-dessus en 6.1.3 b) avec celles de l'Annexe A et vérifier qu'aucune mesure de sécurité nécessaire n'a été omise ;

NOTE 2 L'Annexe A comporte une liste de possibles mesures de sécurité de l'information. Les utilisateurs du présent document sont invités à se reporter à l'Annexe A pour s'assurer qu'aucune mesure de sécurité de l'information nécessaire n'a été négligée.

NOTE 3 Les mesures de sécurité de l'information énumérées dans l'Annexe A ne sont pas exhaustives et des mesures de sécurité de l'information additionnelles peuvent être incluses si nécessaires.

d) produire une déclaration d'applicabilité contenant :

— les mesures de sécurité nécessaires (voir 6.1.3 b) et c)) ;

— la justification de leur insertion ;

— si les mesures de sécurité nécessaires sont mises en œuvre ou non ; et

— la justification de l'exclusion de mesures de sécurité de l'Annexe A ;

e) élaborer un plan de traitement des risques de sécurité de l'information ; et

f) obtenir des propriétaires des risques l'approbation du plan de traitement des risques et l'acceptation des risques résiduels de sécurité de l'information.

L'organisation doit conserver des informations documentées sur le processus de traitement des risques de sécurité de l'information.

NOTE 4 L'appréciation des risques de sécurité de l'information et le processus de traitement figurant dans le présent document s'alignent sur les principes et les lignes directrices générales fournies dans l'ISO 31000[5].

6.2 Objectifs de sécurité de l'information et plans pour les atteindre

L'organisation doit établir, aux fonctions et niveaux concernés, des objectifs de sécurité de l'information.

Les objectifs de sécurité de l'information doivent :

a) être cohérents avec la politique de sécurité de l'information ;

b) être mesurables (si possible) ;

c) tenir compte des exigences applicables à la sécurité de l'information, et des résultats de l'appréciation et du traitement des risques ;

d) être surveillés ;

e) être communiqués ;

f) être mis à jour comme approprié ;