Norme internationale

Redline version compare la Sixième édition à la Cinquième édition

ISO/IEC 27000

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

Information security, cybersecurity and privacy protection — Information security management systems — Overview

Numéro de référence
ISO/IEC 27000:redline:2026(fr)

INFORMATION SUR LA PRÉSENTE VERSION AVEC MARQUES DE RÉVISION

Le présent document est une **version avec marques de révision**, publié à titre informatif. Il a pour objectif d'aider les utilisateurs à identifier les modifications introduites par rapport à l'édition précédente de la norme.

Les ajouts sont mis en évidence en vert.

Les suppressions sont indiquées par un texte barré en rouge.

Pour les éléments graphiques, les ajouts sont signalés par un cadre vert, et les suppressions par une croix rouge.

Les numéros d'articles et de titres contenant des modifications sont surlignés en jaune dans le Sommaire.

La présente version avec marques de révision n'est pas une norme ISO officielle et ne remplace pas l'édition publiée en vigueur. Seule l'édition actuelle de la Norme internationale doit être considérée comme le document officiel.

Marquage utilisé dans la présente version avec marques de révision

Text example 1	texte ajouté (surlignage vert)
~~Text example 2~~	exte supprimé (barré en rouge)
	graphique ajouté (cadre vert)
	graphique supprimé (croix rouge)
1.x ...	numéros d'articles et de titres modifiés (surlignés en jaune dans le Sommaire)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

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
Web: www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) ~~est une fédération mondiale d'organismes nationaux de normalisation (comités~~et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO~~). L'élaboration des Normes internationales est en général confiée aux~~ 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~~. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les~~ 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. ~~L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.~~

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~~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 ne saurait être tenue pour responsable 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).~~

L'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

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 ~~le lien suivant. www.iso.org/avant-propos~~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, ~~*Techniques de sécurité des technologies de l'information*~~*Sécurité de l'information, cybersécurité et protection de la vie privée*, en collaboration avec le comité technique CEN/CLC/JTC 13, *Cybersécurité et protection des données*, du Comité européen de normalisation (CEN), conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette ~~cinquième~~sixième édition annule et remplace la ~~quatrième~~cinquième édition (ISO/IEC 27000:~~2016~~2018), qui a fait l'objet d'une révision technique. ~~Les principales modifications par rapport à l'édition précédente sont les suivantes:~~

Les principales modifications sont les suivantes:

— le titre a été modifié;

~~— modification du texte de l'Introduction;~~

— la structure du document a été modifiée pour souligner son rôle principal, qui est de fournir une vue d'ensemble et d'expliquer les relations entre les documents relatifs au SMSI (systèmes de management de la sécurité de l'information), y compris l'ISO/IEC 27001;

— ~~suppression de certains termes et définitions;~~

— un texte présentant les concepts et les principes de la sécurité de l'information et des systèmes de management de la sécurité de l'information a été ajouté;

— ~~alignement de l'Article 3 par rapport à la structure-cadre pour MSS;~~

— ~~mise à jour de l'Article 5 pour refléter les modifications dans les normes concernées;~~

— l'Article 3 a été modifié afin de contenir uniquement les définitions des termes utilisés pour présenter les concepts et principes décrits dans le présent document;

— ~~suppression des Annexes A et B.~~

— il ne s'agit plus un document terminologique.

Le présent document a obtenu le statut de document transversal conformément aux Directives ISO/IEC, Partie 1.

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 Vue d'ensemble

Les Normes internationales relatives aux systèmes de management fournissent un modèle en matière d'établissement et d'exploitation d'un système de management. Ce modèle comprend les caractéristiques que les experts dans le domaine s'accordent à reconnaître comme reflétant l'état de l'art au niveau international. Le sous-comité ISO/IEC JTC 1/SC 27 bénéficie de l'expérience d'un comité d'experts qui se consacre à l'élaboration des Normes internationales sur les systèmes de management pour la sécurité de l'information, connues également comme famille de normes du Système de Management de la Sécurité de l'Information (SMSI).

Grâce à l'utilisation de la famille de normes du SMSI, les organismes peuvent élaborer et mettre en œuvre un cadre de référence pour gérer la sécurité de leurs actifs informationnels, y compris les informations financières, la propriété intellectuelle, les informations sur les employés, ou les informations qui leur sont confiées par des clients ou des tiers. Ils peuvent également utiliser ces normes pour se préparer à une évaluation indépendante de leur SMSI en matière de protection de l'information.

0.2 Objet du présent document

La famille de normes du SMSI comporte des normes qui:

a) définissent les exigences relatives à un SMSI et à ceux qui certifient de tels systèmes;

b) apportent des informations directes, des recommandations et/ou une interprétation détaillées concernant le processus général visant à établir, mettre en œuvre, maintenir et améliorer un SMSI;

c) présentent des lignes directrices propres à des secteurs particuliers en matière de SMSI;

d) traitent de l'évaluation de la conformité d'un SMSI.

0.3 Contenu du présent document

Dans le présent document, les formes verbales suivantes sont utilisées:

— «doit» indique une exigence;

— «il convient» indique une recommandation;

— «peut» indique une autorisation («may» en anglais);

— ou une possibilité ou une capacité («can» en anglais).

Les informations sous forme de «NOTE» sont fournies pour clarifier l'exigence associée ou en faciliter la compréhension. Les «Notes à l'article» employées à l'Article 3 fournissent des informations supplémentaires qui viennent compléter les données terminologiques et peuvent contenir des dispositions concernant l'usage d'un terme.

Le présent document explique les concepts et les principes qui sous-tendent les systèmes de management de la sécurité de l'information. Il fournit une vue d'ensemble de tous les documents relatifs au SMSI (systèmes de management de la sécurité de l'information), y compris l'ISO/IEC 27001 et explique la relation entre eux.

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

1 Domaine d'application

Le présent document ~~offre~~donne une vue d'ensemble des concepts et des principes utilisés dans des documents relatifs aux systèmes de management de la sécurité de l'information (SMSI)~~. Il comprend également les termes et définitions d'usage courant dans la famille de normes du SMSI. Le présent document est applicable à tous les types et à toutes les tailles d'organismes (par exemple, les entreprises commerciales, les organismes publics, les organismes à but non lucratif)~~, y compris l'ISO/IEC 27001.

~~Les termes et les définitions fournis dans le présent document:~~

~~— couvrent les termes et les définitions d'usage courant dans la famille de normes du SMSI;~~

~~— ne couvrent pas l'ensemble des termes et des définitions utilisés dans la famille de normes du SMSI;~~

~~— ne limitent pas la famille de normes du SMSI en définissant de nouveaux termes à utiliser.~~

Le présent document est pris en considération comme un document transversal, car il explique les concepts et les principes qui sous-tendent la sécurité de l'information et le SMSI.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants 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 ~~http~~ https://www.electropedia.org/

~~**3.1**~~
~~**contrôle d'accès**~~
~~moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les *exigences* (3.56) propres à la sécurité et à l'activité métier~~

~~**3.2**~~
~~**attaque**~~
~~tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'utiliser sans autorisation un actif, ou de faire un usage non autorisé de celui-ci~~

~~3.3~~
3.1
~~audit~~
sécurité de l'information
~~*processus* méthodique, indépendant et documenté (3.54) permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits~~

~~Note 1 à l'article: Un audit peut être interne (audit de première partie), externe (audit de seconde ou de tierce partie) ou combiné (associant deux disciplines ou plus).~~

~~Note 2 à l'article: Un audit interne est réalisé par l'organisme lui-même ou par une partie externe pour le compte de celui-ci.~~

~~Note 3 à l'article: Les termes «preuves d'audit» et «critères d'audit» sont définis dans l'ISO 19011.~~

protection de la *confidentialité* (3.2), de l'*intégrité* (3.3) et de la *disponibilité* (3.4) de l'information

~~3.4~~
3.2
~~champ de l'audit~~
confidentialité
~~étendue et limites d'un *audit* (3.3)~~

~~[SOURCE: ISO 19011:2011, 3.14, modifiée — Suppression de la note 1 à l'article.]~~

propriété d'une information qui n'est ni disponible, ni divulguée aux personnes, entités ou processus non autorisés

~~3.5~~
~~authentification~~
~~méthode permettant de garantir qu'une caractéristique revendiquée pour une entité est correcte~~

~~3.6~~
3.3
~~authenticité~~
intégrité
propriété ~~selon laquelle une entité est ce qu'elle revendique être~~ d'exactitude et de complétude

~~3.7~~
3.4
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

~~3.8~~
~~mesure élémentaire~~
~~*mesure* (3.42) définie en fonction d'un attribut et de la méthode de mesurage spécifiée pour le quantifier~~

~~Note 1 à l'article: Une mesure élémentaire est fonctionnellement indépendante des autres mesures.~~

~~[SOURCE: ISO/IEC/IEEE 15939:2017, 3.3, modifiée — Suppression de la note 2 à l'article.]~~

~~3.9~~
~~compétence~~
~~capacité à appliquer des connaissances et des aptitudes pour obtenir les résultats escomptés~~

~~3.10~~
~~confidentialité~~
~~propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des *processus* (3.54) non autorisés~~

~~3.11~~
~~conformité~~
~~satisfaction d'une *exigence* (3.56)~~

3.12
conséquence
effet d'un *événement* (3.21) affectant les *objectifs* (3.49)

Note 1 à l'article: Un événement peut engendrer une série de conséquences.

Note 2 à l'article: Une conséquence peut être certaine ou incertaine, dans le contexte de la sécurité de l'information, elle est généralement négative.

Note 3 à l'article: Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Note 4 à l'article: Des conséquences initiales peuvent déclencher des réactions en chaîne.

[SOURCE: Guide ISO 73:2009, 3.6.1.3, modifié — Modification de la Note 2 à l'article après «et».]

3.13
amélioration continue
activité régulière destinée à améliorer les *performances* (3.52)

3.14
mesure de sécurité
mesure qui modifie un *risque* (3.61)

Note 1 à l'article: Les mesures de sécurité comprennent tous les *processus* (3.54), *politiques* (3.53), dispositifs, pratiques ou autres actions qui modifient un *risque* (3.61).

Note 2 à l'article: Il est possible que les mesures de sécurité ne puissent pas toujours aboutir à la modification voulue ou supposée.

[SOURCE: Guide ISO 73:2009, 3.8.1.1, — Modification de la Note 2 à l'article.]

3.15
objectif d'une mesure de sécurité
déclaration décrivant ce qui est attendu de la mise en œuvre des *mesures de sécurité* (3.14)

3.16
correction
action visant à éliminer une *non-conformité* (3.47) détectée

3.17
action corrective
action visant à éliminer la cause d'une *non-conformité* (3.47) et à empêcher qu'elle ne se répète

3.18
mesure dérivée
mesure (3.42) définie en fonction d'au moins deux *mesures élémentaires* (3.8)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.8, modifiée — Suppression de la note 1 à l'article.]

3.19
informations documentées
informations devant être contrôlées et mises à jour par un *organisme* (3.50) et le support sur lequel elles sont stockées

Note 1 à l'article: Les informations documentées peuvent être dans n'importe quel format, sur n'importe quel support et provenir de n'importe quelle source.

Note 2 à l'article: Les informations documentées peuvent se rapporter:

— au *système de management* (3.41) et aux *processus* associés (3.54);

— aux informations créées pour permettre à l'*organisme* (3.50) de fonctionner (documentation);

— aux preuves des résultats obtenus (enregistrements).

~~**3.20**~~
~~**efficacité**~~
~~niveau de réalisation des activités planifiées et d'obtention des résultats escomptés~~

~~**3.21**~~
3.5
événement
occurrence ou changement d'un ensemble particulier de circonstances

~~Note 1 à l'article: Un événement peut être unique ou se reproduire. Il peut avoir plusieurs causes.~~

~~Note 2 à l'article: Un événement peut consister en quelque chose qui ne se produit pas.~~

~~Note 3 à l'article: Un événement peut parfois être qualifié «d'incident» ou «d'accident».~~

~~[SOURCE: Guide ISO 73:2009, 3.5.1.3, modifié — Suppression de la note 4 à l'article.]~~

[SOURCE: ISO/IEC 27005:2022, 3.1.11, modifié — Les Notes à l'article ont été omises.]

~~**3.22**~~
~~**contexte externe**~~
~~environnement externe dans lequel l'organisme cherche à atteindre ses *objectifs* (3.49)~~

~~Note 1 à l'article: Le contexte externe peut inclure les aspects suivants:~~

~~— l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local;~~

~~— *les facteurs clés et tendances ayant un impact déterminant sur les objectifs* de l'organisme (3.50);~~

~~— les relations avec les *parties prenantes* (3.37) externes, les perceptions et valeurs relatives à celles-ci.~~

~~[SOURCE: Guide ISO 73:2009, 3.3.1.1]~~

~~**3.23**~~
~~**gouvernance de la sécurité de l'information**~~
~~système par lequel un *organisme* (3.50) conduit et supervise les activités liées à la *sécurité de l'information* (3.28)~~

~~**3.24**~~
~~**instances dirigeantes**~~
~~personne ou groupe de personnes ayant la responsabilité des *performances* (3.52) et de la conformité de l'*organisme* (3.50)~~

~~Note 1 à l'article: Dans certaines juridictions, les instances dirigeantes peuvent être constituées d'un conseil d'administration.~~

~~**3.25**~~
~~**indicateur**~~
~~*mesure* (3.42) qui fournit une estimation ou une évaluation~~

~~**3.26**~~
~~**besoin d'information**~~
~~information nécessaire pour gérer les *objectifs* (3.49), les buts, les risques et les problèmes~~

~~[SOURCE: ISO/IEC/IEEE 15939:2017, 3.12]~~

~~**3.27**~~
~~**moyens de traitement de l'information**~~
~~tout système, service ou infrastructure de traitement de l'information, ou le local les abritant~~