NORME INTERNATIONALE

ISO/IEC 27000

Cinquième édition
2018-02

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

Information technology — Security techniques — Information security management systems — Overview and vocabulary

Numéro de référence
ISO/IEC 27000:2018(F)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
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 membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux 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 organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO 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).

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).

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.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, SC 27, *Techniques de sécurité des technologies de l'information*.

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

— modification du texte de l'Introduction;

— suppression de certains termes et définitions;

— 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;

— suppression des Annexes A et B.

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.

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire

1 Domaine d'application

Le présent document offre une vue d'ensemble des 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).

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.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes et definitions

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://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
audit
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.

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

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

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

3.6
authenticité
propriété selon laquelle une entité est ce qu'elle revendique être

3.7
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
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.]

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

3.28
sécurité de l'information
protection de la *confidentialité* (3.10), de l'*intégrité* (3.36) et de la *disponibilité* (3.7) de l'information

Note 1 à l'article: En outre, d'autres propriétés, telles que *l'authenticité* (3.6), l'imputabilité, la *non-répudiation* (3.48) et la *fiabilité* (3.55) peuvent également être concernées.

3.29
continuité de la sécurité de l'information
processus (3.54) et procédures visant à assurer la continuité des opérations liées à la *sécurité de l'information* (3.28)

3.30
événement lié à la sécurité de l'information
occurrence identifiée de l'état d'un système, d'un service ou d'un réseau indiquant une faille possible dans la *politique* (3.28) de sécurité de l'*information* (3.53) ou un échec des *mesures de sécurité* (3.14), ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité

3.31
incident lié à la sécurité de l'information
un ou plusieurs *événements liés à la sécurité de l'information* (3.30), indésirables ou inattendus, présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la *sécurité de l'information* (3.28)

3.32
gestion des incidents liés à la sécurité de l'information
ensemble de *processus* (3.54) visant à détecter, rapporter, apprécier, gérer et résoudre les *incidents liés à la sécurité de l'information* (3.31), ainsi qu'à en tirer des enseignements

3.33
professionnel SMSI (Système de management de la sécurité de l'information)
personne chargée d'établir et de mettre en œuvre un ou plusieurs *processus* (3.54) d'un système de management de la sécurité de l'information, ainsi que d'en assurer la maintenance et l'amélioration continue

3.34
communauté de partage d'informations
groupe d'*organismes* (3.50) qui s'accordent pour partager des informations

Note 1 à l'article: Un organisme peut être un individu.

3.35
système d'information
ensemble d'applications, services, actifs informationnels ou autres composants permettant de gérer l'information

3.36
intégrité
propriété d'exactitude et de complétude

3.37
partie intéressée (terme préféré)
partie prenante (terme admis)
personne ou *organisme* (3.50) susceptible d'affecter, d'être affecté ou de se sentir lui-même affecté par une décision ou une activité

3.38
contexte interne
environnement interne dans lequel l'*organisme* (3.50) cherche à atteindre ses objectifs

Note 1 à l'article: Le contexte interne peut inclure:

— la gouvernance, la structure organisationnelle, les rôles et les responsabilités;

— *les politiques* (3.53), *objectifs* (3.49) et stratégies mises en place pour atteindre ces derniers;

— les capacités, en termes de ressources et de connaissances (par exemple: capital, temps, personnel, *processus* (3.54), systèmes et technologies);

— *les systèmes d'information* (3.35), flux d'information et *processus* de prise de décision (formels et informels);

— les relations avec les *parties prenantes* (3.37) internes, les perceptions et valeurs associées à celles-ci;

— la culture de l'organisme;

— les normes, lignes directrices et modèles adoptés par l'*organisme*;

— la forme et l'étendue des relations contractuelles.

[SOURCE: Guide ISO 73:2009, 3.3.1.2]

3.39
niveau de risque
importance d'un *risque* (3.61) exprimée en termes de combinaison des *conséquences* (3.12) et de leur *vraisemblance* (3.40)

[SOURCE: Guide ISO 73:2009, 3.6.1.8, modifiée— Suppression de «ou combinaison de risques» de la définition.]

3.40
vraisemblance
possibilité que quelque chose se produise

[SOURCE: Guide ISO 73:2009, 3.6.1.1, modifié — Suppression des notes 1 et 2 à l'article.]

3.41
système de management
ensemble d'éléments corrélés ou interactifs d'un *organisme* (3.50) visant à établir des *politiques* (3.53), des *objectifs* (3.49) et des *processus* (3.54) permettant d'atteindre ces objectifs

Note 1 à l'article: Un système de management peut recouvrir une ou plusieurs disciplines.

Note 2 à l'article: Les éléments du système comprennent la structure de l'organisme, les rôles et responsabilités, la planification et les opérations.

Note 3 à l'article: Le domaine d'un système de management peut comprendre l'organisme dans son ensemble, certaines de ses fonctions spécifiques et identifiées, certaines de ses sections spécifiques et identifiées, ou une ou plusieurs fonctions au sein d'un groupe d'organismes.

3.42
mesure
variable à laquelle on attribue une valeur correspondant au résultat du *mesurage* (3.43)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.15, modifiée — Suppression de la note 2 à l'article.]

3.43
mesurage
processus (3.54) permettant de déterminer une valeur

3.44
fonction de mesurage
algorithme ou calcul utilisé pour combiner au moins deux *mesures élémentaires* (3.8)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.20]

3.45
méthode de mesurage
suite logique d'opérations décrites de manière générique qui permettent de quantifier un attribut selon une échelle spécifiée

Note 1 à l'article: Le type de méthode de mesure employé dépend de la nature des opérations utilisées pour quantifier un *attribut* (3.4). On peut en distinguer deux:

— le type subjectif: quantification faisant appel au jugement humain;

— le type objectif: quantification fondée sur des règles numériques.

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.21, modifiée — Suppression de la note 2 à l'article.]

