NORME INTERNATIONALE

ISO/CEI 27000

Troisième édition
2014-01-15

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/CEI 27000:2014(F)

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

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 à l'élaboration de Normes internationales par l'intermédiaire de comités techniques créés par l'organisme concerné pour traiter de domaines particuliers à une activité technique de leur compétence. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organismes internationaux, gouvernementaux et non gouvernementaux, en liaison avec l'ISO et l'IEC participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte: l'ISO/IEC JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale du comité technique mixte est d'élaborer des Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication en tant que Normes internationales requiert l'approbation d'au moins 75 % des organismes nationaux votants.

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. 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.

L'ISO/IEC 27000 a été élaborée 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*.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27000:2012), qui a fait l'objet d'une révision technique.

0 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. Elles peuvent également utiliser ces normes pour se préparer à une évaluation indépendante de leurs SMSI en matière de protection de l'information.

0.2 La famille de normes du SMSI

La famille de normes du SMSI (voir l'Article 4) a pour objet d'aider les organismes de tous types et de toutes tailles à déployer et à exploiter un SMSI. Elle se compose des Normes internationales suivantes (indiquées ci-dessous par ordre numérique) regroupées sous le titre général *Technologies de l'information — Techniques de sécurité*:

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

— ISO/IEC 27001, *Systèmes de management de la sécurité de l'information — Exigences*

— ISO/IEC 27002, *Code de bonne pratique pour les mesures de sécurité de l'information*

— ISO/IEC 27003, *Lignes directrices pour la mise en oeuvre du système de management de la sécurité de l'information*

— ISO/IEC 27004, *Management de la sécurité de l'information — Mesurage*

— ISO/IEC 27005, *Gestion des risques liés à la sécurité de l'information*

— ISO/IEC 27006, *Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information*

— ISO/IEC 27007, *Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information*

— ISO/IEC/TR 27008, *Lignes directrices pour les auditeurs des contrôles de sécurité de l'information*

— ISO/IEC 27010, *Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles*

— ISO/IEC 27011, *Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'*ISO/IEC 27002

— ISO/IEC 27013, *Guide sur la mise en oeuvre intégrée de* l'ISO/IEC 27001 *et de l'*ISO/IEC 20000-1

— ISO/IEC 27014, *Gouvernance de la sécurité de l'information*

— ISO/IEC/TR 27015, *Lignes directrices pour le management de la sécurité de l'information pour les services financiers*

— ISO/IEC/TR 27016, *Management de la sécurité de l'information — Économie organisationnelle*

NOTE Le titre général «*Technologies de l'information — Techniques de sécurité*» indique que ces normes ont été élaborées 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*.

Les Normes internationales qui font également partie de la famille de normes du SMSI, mais qui ne sont pas regroupées sous le même titre général, sont les suivantes:

— ISO 27799:2008, *Informatique de santé — Gestion de la sécurité de l'information relative à la santé en utilisant l'*ISO/IEC 27002

0.3 Objet de la présente Norme internationale

La présente Norme internationale offre une vue d'ensemble des systèmes de management de la sécurité de l'information et définit les termes qui s'y rapportent.

NOTE L'Annexe A fournit des éclaircissements sur la façon dont les formes verbales sont utilisées pour exprimer des exigences et/ou des préconisations dans la famille de normes du SMSI.

La famille de normes du SMSI comporte des normes qui:

a) définissent les exigences pour un SMSI et pour les organismes certifiant de tels systèmes;

b) apportent un soutien direct, des préconisations détaillées et/ou une interprétation du processus général visant à établir, mettre en œuvre, entretenir et améliorer un SMSI;

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

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

Les termes et les définitions fournis dans la présente Norme internationale:

— 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.

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

La présente Norme internationale offre une vue d'ensemble des systèmes de management de la sécurité de l'information, et des termes et définitions d'usage courant dans la famille de normes du SMSI. La présente Norme internationale 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).

2 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

2.1
contrôle d'accès
moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les exigences propres à la sécurité et à l'activité métier

2.2
modèle analytique
algorithme ou calcul combinant une ou plusieurs *mesures élémentaires (2.10)* et/ou *mesures dérivées* (2.22) avec les critères de décision associés

2.3
attaque
tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'obtenir un accès non autorisé ou d'utiliser sans autorisation un actif

2.4
attribut
propriété ou caractéristique d'un *objet* (2.55) qui peut être distingué quantitativement ou qualitativement par des moyens humains ou automatiques

[SOURCE: ISO/IEC 15939:2007, modifiée – le terme «entité» a été remplacé par «objet» dans la définition.]

2.5
audit
processus méthodique, indépendant et documenté (2.61) 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) ou externe (audit de seconde ou de tierce partie), et peut également être un audit combiné (combinant deux disciplines ou plus).

Note 2 à l'article: Les termes «preuves d'audit» et «critères d'audit» sont définis dans l'ISO 19011.

2.6
champ de l'audit
étendue et limites d'un *audit* (2.5)

[SOURCE: ISO 19011:2011]

2.7
authentification
moyen pour une entité d'assurer la légitimité d'une caractéristique revendiquée

2.8
authenticité
propriété selon laquelle une entité est ce qu'elle revendique être

2.9
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

2.10
mesure élémentaire
mesure (2.47) définie en fonction d'un *attribut* (2.4) et de la méthode de mesurage spécifiée pour le quantifier

[SOURCE: ISO/IEC 15939:2007]

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

2.11
compétence
aptitude à mettre en œuvre des connaissances et savoir-faire en vue d'obtenir des résultats prévus

2.12
confidentialité
propriété selon laquelle l'information n'est pas rendue disponible ni divulguée à des personnes, des entités ou des *processus* (2.61) non autorisés

2.13
conformité
satisfaction d'une *exigence* (2.63)

Note 1 à l'article: Le terme anglais «conformance» est un synonyme mais a été abandonné.

2.14
conséquence
effet d'un *événement* (2.25) affectant les *objectifs* (2.56)

[SOURCE: Guide ISO 73:2009]

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.

2.15
amélioration continue
activité régulière destinée à améliorer les *performances* (2.59)

2.16
mesure de sécurité
mesure qui modifie un *risque* (2.68)

[SOURCE: Guide ISO 73:2009]

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

Note 2 à l'article: Les mesures de sécurité ne peuvent pas toujours aboutir à la modification voulue ou supposée.

2.17
objectif de sécurité
déclaration décrivant ce qui doit être atteint comme résultat de la mise en œuvre des *mesures de sécurité* (2.16)

2.18
correction
action visant à éliminer une *non-conformité* (2.53) détectée

2.19
action corrective
action visant à éliminer la cause d'une *non-conformité* (2.53) et à empêcher sa répétition

2.20
données
ensemble des valeurs attribuées aux *mesures élémentaires* (2.10), aux *mesures dérivées* (2.22) et/ou aux *indicateurs* (2.30)

[SOURCE: ISO/IEC 15939:2007]

Note 1 à l'article: Cette définition s'applique uniquement dans le contexte de l'ISO/IEC 27004:2009.

2.21
critères de décision
seuils, cibles ou modèles utilisés pour déterminer la nécessité d'une action ou d'un complément d'enquête, ou pour décrire le niveau de confiance dans un résultat donné

[SOURCE: ISO/IEC 15939:2007]

2.22
mesure dérivée
mesure (2.47) définie en fonction d'au moins deux *mesures élémentaires* (2.10)

[SOURCE: ISO/IEC 15939:2007]

2.23
informations documentées
informations devant être contrôlées et mises à jour par un *organisme* (2.57) et le support sur lequel elles sont contenues

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* (2.46) et aux *processus associés* (2.61);

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

— aux preuves des résultats obtenus (enregistrements).

2.24
efficacité
niveau de réalisation des activités planifiées et d'obtention des résultats escomptés

2.25
événement
occurrence ou changement d'un ensemble particulier de circonstances

[SOURCE: Guide ISO 73:2009]

Note 1 à l'article: Un événement peut être unique ou se reproduire et 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».

2.26
management exécutif
personne ou groupe de personnes ayant reçu des *instances dirigeantes* (2.29) la responsabilité de la mise en œuvre des stratégies et politiques afin de réaliser les objectifs de *l'organisme* (2.57)

Note 1 à l'article: Le management exécutif est parfois appelé la direction, et peut comprendre les Directeurs, les Responsables des Finances, les Responsables de l'Information, et autres fonctions similaires

2.27
contexte externe
environnement externe dans lequel l'organisme cherche à atteindre ses objectifs

[SOURCE: Guide ISO 73:2009]

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

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

— les facteurs et tendances ayant un impact déterminant sur les *objectifs* (2.56) de *l'organisme* (2.57);

— les relations avec les *parties prenantes* (2.82) externes, leurs perceptions et leurs valeurs.

2.28
gouvernance de la sécurité de l'information
système au moyen duquel un *organisme* (2.57) oriente et supervise les activités liées à la sécurité de l'information

2.29
instances dirigeantes
personne ou groupe de personnes ayant la responsabilité des *performances* (2.59) et de la conformité de *l'organisme* (2.57)

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

2.30
indicateur
mesure (2.47) qui fournit une estimation ou une évaluation *d'attributs* (2.4) spécifiés à partir d'un *modèle analytique* (2.2) concernant des *besoins d'information* (2.31) définis

2.31
besoin d'information
information nécessaire pour gérer les objectifs, les risques et les problèmes

[SOURCE: ISO/IEC 15939:2007]

2.32
moyens de traitement de l'information
tout système, service ou infrastructure de traitement de l'information, ou local les abritant

2.33
sécurité de l'information
protection de la *confidentialité* (2.12), de *l'intégrité* (2.40) et de la *disponibilité* (2.9) de l'information

Note 1 à l'article: En outre, d'autres propriétés, telles que *l'authenticité* (2.8), l'imputabilité, la *non-répudiation* (2.54) et la *fiabilité* (2.62) peuvent également être concernées.

2.34
continuité de la sécurité de l'information
processus (2.61) et procédures visant à assurer la continuité des opérations liées à la *sécurité de l'information* (2.33)

2.35
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 de sécurité de l'information ou un échec des mesures de sécurité, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité

2.36
incident lié à la sécurité de l'information
un ou plusieurs *événements liés à la sécurité de l'information* (2.35) 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* (2.33)

2.37
gestion des incidents liés à la sécurité de l'information
processus (2.61) pour détecter, rapporter, apprécier, intervenir, résoudre et tirer les enseignements des *incidents liés à la sécurité de l'information* (2.36)

2.38
communauté de partage d'informations
groupe d'organismes qui s'accordent pour partager les informations

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

2.39
système d'information
applications, services, actifs informationnels ou autre composante permettant la prise en charge de l'information

2.40
intégrité
propriété d'exactitude et de complétude

2.41
partie intéressée
personne ou *organisme* (2.57) susceptible d'affecter, d'être affectée ou de se sentir elle-même affectée par une décision ou une activité

2.42
contexte interne
environnement interne dans lequel l'organisme cherche à atteindre ses objectifs

[SOURCE: Guide ISO 73:2009]

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

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

— les politiques, les objectifs et les stratégies mises en place pour atteindre ces derniers;

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

— les systèmes d'information, les flux d'information et les processus de prise de décision (à la fois formels et informels);

— les relations avec les parties prenantes internes, ainsi que leurs perceptions et leurs valeurs;

— la culture de l'organisme;

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

— la forme et l'étendue des relations contractuelles.

2.43
projet SMSI
activités structurées entreprises par un *organisme* (2.57) pour déployer un SMSI

2.44
niveau de risque
importance d'un *risque* (2.68) exprimée en termes de combinaison des *conséquences* (2.14) et de leur *vraisemblance* (2.45)

[SOURCE: Guide ISO 73:2009, modifié – l'expression «ou combinaison de risques» a été supprimée.]

2.45
vraisemblance
possibilité que quelque chose se produise

[SOURCE: Guide ISO 73:2009]

2.46
système de management
ensemble d'éléments corrélés ou interactifs d'un *organisme* (2.57) visant à établir des *politiques* (2.60), des *objectifs* (2.56) et des *processus* (2.61) afin 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, les opérations, etc.

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.

2.47
mesure
variable à laquelle on attribue une valeur correspondant au résultat du *mesurage* (2.48)

[SOURCE: ISO/IEC 15939:2007]

Note 1 à l'article: Le terme «mesures» est utilisé pour désigner collectivement les mesures élémentaires, les mesures dérivées et les indicateurs.

2.48
mesurage
processus (2.61) permettant de déterminer une valeur

Note 1 à l'article: Dans le contexte de la *sécurité de l'information* (2.33), le processus de détermination d'une valeur nécessite des informations concernant *l'efficacité* (2.24) d'un *système de management* (2.46) de la sécurité de l'information et de ses *mesures de sécurité* (2.16) associées à l'aide d'une *méthode de mesurage* (2.50), d'une *fonction de mesurage* (2.49), d'un *modèle analytique* (2.2) et de *critères de décision* (2.21).

2.49
fonction de mesurage
algorithme ou calcul utilisé pour combiner au moins deux *mesures élémentaires* (2.10)

[SOURCE: ISO/IEC 15939:2007]

2.50
méthode de mesurage
suite logique d'opérations décrites de manière générique qui permettent de quantifier un *attribut* (2.4) selon une *échelle* (2.80) spécifiée

[SOURCE: ISO/IEC 15939:2007]

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

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

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

2.51
résultats de mesurage
un ou plusieurs *indicateurs* (2.30), et les interprétations associées, répondant à un *besoin d'information* (2.31)

2.52
surveillance
détermination du statut d'un système, d'un *processus* (2.61) ou d'une activité

Note 1 à l'article: Pour déterminer le statut, il peut s'avérer nécessaire de vérifier, de superviser ou d'observer de manière critique.

2.53
non-conformité
non-satisfaction d'une *exigence* (2.63)

2.54
non-répudiation
capacité à prouver l'occurrence d'un événement ou d'une action donné(e) et des entités qui en sont à l'origine

2.55
objet
élément caractérisé par le *mesurage* (2.48) de ses *attributs* (2.4)

2.56
objectif
résultat à atteindre

Note 1 à l'article: Un objectif peut être stratégique, tactique ou opérationnel.

Note 2 à l'article: Les objectifs peuvent se rapporter à différentes disciplines (par exemple: buts financiers, de santé et de sécurité, ou environnementaux) et peuvent concerner différents niveaux (par exemple: au niveau stratégique, à l'échelle de l'organisme, au niveau d'un projet, d'un produit et d'un **processus**) [2.61]).

Note 3 à l'article: Un objectif peut être exprimé de différentes manières, par exemple comme un résultat recherché, un but, un critère opérationnel, un objectif de sécurité de l'information, ou en utilisant d'autres mots de sens similaire (par exemple: intention ou cible).

Note 4 à l'article: Dans le contexte des systèmes de management de la sécurité de l'information, les objectifs de sécurité de l'information sont établis par l'organisme, conformément à la politique de sécurité de l'information, afin d'obtenir des résultats spécifiques.