NORME INTERNATIONALE

ISO/CEI 27000

Première édition
2009-05-01

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 27000:2009(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

Version française parue en 2010

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI 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 la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

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

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins 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 la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27000 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

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/CEI 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 des Systèmes de Management de la Sécurité de l'Information (SMSI).

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

0.2 La famille de normes du SMSI

La famille de normes du SMSI[1)] a pour objet d'aider les organisations de tous types et de toutes tailles à déployer et exploiter un SMSI. Dans le domaine des «*Technologies de l'information — Techniques de sécurité*», le titre général de chacune des normes du SMSI se présente comme suit:

— ISO/CEI 27000:2009, *Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

— ISO/CEI 27001:2005, *Systèmes de management de la sécurité de l'information — Exigences*

— ISO/CEI 27002:2005, *Code de bonne pratique pour le management de la sécurité de l'information*

— ISO/CEI 27003, *Guide de mise en œuvre du système de management de la sécurité de l'information*

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

— ISO/CEI 27005:2008, *Management du risque de la sécurité de l'information*

— ISO/CEI 27006:2007, *Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information*

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

— ISO/CEI 27011:2008, *Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002*

NOTE Le titre général «Technologies de l'information – Techniques de sécurité» indique que ces normes ont été élaborées par le comité technique mixte ISO/CEI JTC 1, Technologies de l'information, sous-comité SC 27, Techniques de sécurité.

---

1) Les normes mentionnées dans cette section qui ne comportent pas d'année de publication sont toujours en cours d'élaboration.

Les Normes internationales qui font également partie de la famille de normes du SMSI, mais qui ne sont pas comprises comme «Technologies de l'information – Techniques de sécurité» sont les suivantes:

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

0.3 Objet de la présente Norme internationale

L'ISO/CEI 27000 présente une vue d'ensemble des systèmes de management de la sécurité de l'information, qui constituent l'objet de la famille de normes du SMSI, et définit les termes qui s'y rapportent.

NOTE L'Annexe A fournit des éclaircissements sur la façon dont les normes de la famille SMSI doivent être interprétées en fonction des expressions verbales utilisées, celles-ci exprimant des exigences et/ou des lignes directrices.

La famille de normes du SMSI comporte des normes qui:

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

b) apportent un soutien direct, des recommandations détaillées et/ou une interprétation des processus et des exigences générales selon le modèle Planifier-Déployer-Contrôler-Agir (PDCA);

c) traitent des pratiques 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 cette Norme internationale:

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

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

c) ne limitent pas la famille de normes du SMSI en définissant des termes pour un usage propre.

Les normes ne traitant que de la mise en œuvre des mesures, par opposition au traitement de l'ensemble des mesures prévu dans l'ISO/CEI 27002, sont exclues de la famille de normes du SMSI.

L'ISO/CEI 27000 est une norme délivrée gratuitement.

Pour tenir compte des fréquentes évolutions de la famille de normes du SMSI, on s'attend à ce que l'ISO/CEI 27000 soit remise à jour en permanence et sur une base plus fréquente que celle prévue pour les autres normes ISO/CEI.

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 fournit:

a) une vue d'ensemble de la famille de normes du SMSI;

b) une introduction aux systèmes de management de la sécurité de l'information (SMSI);

c) une brève description du processus Planifier-Déployer-Contrôler-Agir (PDCA); et

d) les termes et définitions utilisés dans la famille de normes du SMSI.

La présente Norme internationale est applicable à tous les types d'organisations (par exemple: entreprises commerciales, organisations publiques, organisations à but non lucratif).

2 Termes et définitions

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

Si ces termes et ces définitions s'appliquent également à d'autres documents, cela doit être indiqué dans ces autres documents à l'aide de l'alinéa d'introduction suivant:

Pour les besoins du présent document, les termes et définitions fournis dans l'ISO/CEI 27000 s'appliquent.

Un terme utilisé dans une définition ou une note et défini à un autre endroit du présent article figure en caractères gras, suivi de la référence de l'entrée entre parenthèses. Ce terme en caractères gras peut être remplacé dans la définition ou la note par sa propre définition.

Par exemple:

attaque (2.4) est définie comme une «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** (2.3)»;

actif est défini comme «tout élément représentant de la valeur pour l'organisation».

En remplaçant le terme «**actif**» par sa définition, on obtient:

attaque est alors définie comme une «tentative de détruire, de rendre public, de modifier, d'invalider, de voler, d'obtenir un accès non autorisé ou d'utiliser sans autorisation tout élément représentant de la valeur pour l'organisation».

2.1
contrôle d'accès
moyens mis en œuvre pour assurer que l'accès aux **actifs** (2.3) est autorisé et limité selon les exigences propres à la sécurité et à l'activité métier

2.2
imputabilité
responsabilité d'une entité par rapport à ses actions et ses décisions

2.3
actif
tout élément représentant de la valeur pour l'organisation

NOTE Il existe plusieurs sortes d'actifs, dont:

(a) l'**information** (2.18);
(b) les logiciels, par exemple un programme informatique;
(c) les actifs physiques, par exemple un ordinateur;
(d) les services;
(e) le personnel, et leurs qualifications, compétences et expérience;
(f) les actifs incorporels, par exemple la réputation et l'image.

2.4
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 (2.3)

2.5
authentification
moyen pour une entité d'assurer la légitimité d'une caractéristique revendiquée

2.6
authenticité
propriété selon laquelle une entité est ce qu'elle revendique être

2.7
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

2.8
continuité de l'activité
processus (2.31) et/ou **procédures** (2.30) permettant d'assurer la continuité de l'activité métier

2.9
confidentialité
propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou des **processus** (2.31) non autorisés

2.10
mesure de sécurité
moyens de gestion des **risques** (2.34), comprenant les **politiques** (2.28), les **procédures** (2.30), les lignes directrices (2.16), les pratiques ou l'organisation, qui peuvent être de nature administrative, technique, manégériale ou juridique

NOTE Mesure de sécurité est également synonyme de protection ou de contre-mesure.

2.11
objectif de sécurité
déclaration décrivant ce qui doit être atteint comme résultat de la mise en oeuvre des **mesures de sécurité** (2.10)

2.12
action corrective
action visant à éliminer la cause d'une non-conformité ou d'une autre situation indésirable détectée

[ISO 9000:2005]

2.13
efficacité
niveau de réalisation des activités planifiées et d'obtention des résultats escomptés

[ISO 9000:2005]

2.14
efficience
rapport entre le résultat obtenu et les ressources utilisées

2.15
événement
occurrence d'un ensemble particulier de circonstances

[ISO/CEI Guide 73:2002]

2.16
ligne directrice
recommandation de ce qui doit être fait pour atteindre un objectif

2.17
impact
altération préjudiciable à la réalisation des objectifs métiers

2.18
actif informationnel
savoir ou données représentant de la valeur pour l'organisation

2.19
sécurité de l'information
protection de la **confidentialité** (2.9), de l'**intégrité** (2.25) et de la **disponibilité** (2.7) de l'information; en outre, d'autres propriétés, telles que l'**authenticité** (2.6), l'**imputabilité** (2.2), la **non-répudiation** (2.27) et la **fiabilité** (2.33), peuvent également être concernées

2.20
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** (2.28) de **sécurité de l'information** (2.19) ou un échec des **mesures de sécurité** (2.10) ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité

2.21
incident lié à la sécurité de l'information
un ou plusieurs **événements liés à la sécurité de l'information** (2.20) indésirables ou inattendus présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisation et de menacer la **sécurité de l'information** (2.19)

2.22
gestion des incidents liés à la sécurité de l'information
processus (2.31) pour détecter, rapporter, apprécier, intervenir, résoudre et tirer les enseignements des **incidents liés à la sécurité de l'information** (2.21)

2.23
système de management de la sécurité de l'information
SMSI
partie du **système de management** global (2.26), basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la **sécurité de l'information** (2.19)

2.24
risque lié à la sécurité de l'information
possibilité qu'une **menace** (2.45) exploite une **vulnérabilité** (2.46) d'un **actif** (2.3) ou d'un groupe d'actifs et nuise donc à l'organisation

2.25
intégrité
propriété de protection de l'exactitude et de la complétude des **actifs** (2.3)

2.26
système de management
cadre de référence des **politiques** (2.28), **procédures** (2.30), **lignes directrices** (2.16) et ressources associées pour atteindre les objectifs de l'organisation

2.27
non-répudiation
capacité à prouver l'occurrence d'un **événement** (2.15) ou d'une action donné et les entités qui en sont à l'origine, de manière à résoudre les litiges entre l'occurrence ou la non-occurrence de **l'événement** (2.15) ou de l'action et l'implication des entités dans l'**événement** (2.15)

2.28
politique
orientations et intentions globales d'une organisation telles qu'elles sont exprimées formellement par la direction

2.29
action préventive
action visant à éliminer la cause d'une non-conformité potentielle ou d'une autre situation potentielle indésirable

[ISO 9000:2005]

2.30
procédure
manière spécifiée d'effectuer une activité ou un **processus** (2.31)

[ISO 9000:2005]

2.31
processus
ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie

[ISO 9000:2005]

2.32
enregistrement
document faisant état de résultats obtenus ou apportant la preuve de la réalisation d'une activité

[ISO 9000:2005]

2.33
fiabilité
propriété relative à un comportement et des résultats prévus et cohérents

2.34
risque
combinaison de la probabilité d'un **événement** (2.15) et de ses conséquences

[Guide ISO/CEI 73:2002]

2.35
acceptation des risques
décision d'accepter un **risque** (2.34)

[Guide ISO/CEI 73:2002]

2.36
analyse des risques
utilisation systématique d'informations pour identifier les sources et pour estimer le **risque** (2.34)

[Guide ISO/CEI 73:2002]

NOTE L'analyse des risques fournit une base pour l'**évaluation des risques** (2.41), le **traitement des risques** (2.43) et l'**acceptation des risques** (2.35)

2.37
appréciation des risques
ensemble du **processus** (2.31) d'**analyse des risques** (2.36) et d'**évaluation des risques** (2.41)

[Guide ISO/CEI 73:2002]

2.38
communication relative aux risques
échange ou partage d'informations concernant le **risque** (2.34) entre le décideur et d'autres parties prenantes

[Guide ISO/CEI 73:2002]

2.39
critères de risque
termes de référence permettant d'apprécier l'importance des **risques** (2.34)

[Guide ISO/CEI 73:2002]

2.40
estimation des risques
activité consistant à affecter des valeurs à la probabilité et aux conséquences d'un **risque** (2.34)

[Guide ISO/CEI 73:2002]

2.41
évaluation des risques
processus (2.31) de comparaison du **risque** (2.34) estimé avec des **critères de risque** (2.39) donnés pour déterminer l'importance du **risque** (2.34)

[Guide ISO/CEI 73:2002]

2.42
gestion du risque
activités coordonnées visant à diriger et contrôler une organisation vis-à-vis du **risque** (2.34)

[Guide ISO/CEI 73:2002]

NOTE La gestion du risque comporte généralement l'**appréciation des risques** (2.37), le **traitement des risques** (2.43), l'**acceptation des risques** (2.35), la **communication relative aux risques** (2.38), la surveillance et le réexamen du risque.