NORME INTERNATIONALE

ISO/CEI 27000

Deuxième édition
2012-12-01

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 27000:2012(F)

Version française parue en 2013

Publié en Suisse

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*.

Cette deuxième édition annule et remplace la première édition (ISO/CEI 27000:2009).

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, y compris 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. 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[1)] du SMSI (voir l'Article 4) a pour objet d'aider les organisations 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/CEI 27000:2009, *Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire*

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

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

— ISO/CEI 27003:2010, *Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information*

— ISO/CEI 27004:2009, *Management de la sécurité de l'information – Mesurage*

— ISO/CEI 27005:2011, *Gestion des risques liés à la sécurité de l'information*

— ISO/CEI 27006:2011, *Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information*

— ISO/CEI 27007:2011, *Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information*

— ISO/CEI TR 27008:2011, *Lignes directrices pour les auditeurs des contrôles de sécurité de l'information*

— ISO/CEI 27010:2012, *Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles*

— ITU-T X.1051 | ISO/CEI 27011:2008, *Lignes directrices pour le management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'ISO/CEI 27002*

---

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

— ISO/CEI FDIS 27013, *Lignes directrices relatives à la mise en œuvre intégrée de l'ISO/CEI 27001 et de l'ISO/CEI 20000-1*

— ITU-T X.1054 | ISO/CEI FDIS 27014, *Gouvernance de la sécurité de l'information*

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

— ISO/CEI WD 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/CEI 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 comprises comme « Technologies de l'information – Techniques de sécurité » sont les suivantes :

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

0.3 Objet de la présente Norme internationale

La présente Norme internationale fournit 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 normes de la famille du 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 généraux 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 :

— 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 décrit une vue d'ensemble et le vocabulaire 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 et les définitions qui s'y rapportent.

La présente Norme internationale est applicable à tous les types et à toutes les tailles 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.

NOTE 1 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 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 :

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** (2.4) est autorisé et limité selon les exigences propres à la sécurité et à l'activité métier

2.2
imputabilité
attribution d'actions et de décisions à une entité

2.3
modèle analytique
algorithme ou calcul combinant une ou plusieurs **mesures élémentaires** (2.11) et/ou **mesures dérivées** (2.21) avec les critères de décision associés

[ISO/CEI 15939:2007]

2.4
actif
tout élément représentant de la valeur pour l'organisation

NOTE Il existe plusieurs sortes d'actifs, dont :

a) l'information ;

b) les logiciels, par exemple un programme informatique ;

c) les actifs physiques, par exemple un ordinateur ;

d) les services ;

e) le personnel, et ses qualifications, compétences et expérience ;

f) les actifs incorporels, par exemple la réputation et l'image.

2.5
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)

2.6
attribut
propriété ou caractéristique d'un objet qui peut être distingué quantitativement ou qualitativement par des moyens humains ou automatiques

[ISO/CEI 15939:2007]

2.7
champ de l'audit
étendue et limites d'un audit

[ISO 9000:2005]

2.8
authentification
moyen pour une entité d'assurer la légitimité d'une caractéristique revendiquée

2.9
authenticité
propriété selon laquelle une entité est ce qu'elle revendique être

2.10
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

2.11
mesure élémentaire
mesure (2.43) définie en fonction d'un **attribut** (2.6) et de la méthode de mesurage spécifiée pour l'identifier

[ISO/CEI 15939:2007]

NOTE Une mesure élémentaire est fonctionnellement indépendante des autres mesures.

2.12
continuité de l'activité
procédures (2.53) et/ou **processus** (2.54) permettant d'assurer la continuité de l'activité métier

2.13
confidentialité
propriété selon laquelle l'information n'est pas rendue disponible ou divulguée à des personnes, des entités ou des **processus** (2.54) non autorisés

2.14
conformité
satisfaction d'une exigence

[ISO 9000:2005]

NOTE Le terme anglais « conformance » est synonyme de « conformity », mais a été abandonné.

2.15
conséquence
effet d'un **événement** (2.24) affectant les objectifs

[Guide ISO 73:2009]

NOTE 1 Un événement peut engendrer une série de conséquences.

NOTE 2 Une conséquence peut être certaine ou incertaine ; dans le contexte de la sécurité de l'information, elle est généralement négative.

NOTE 3 Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

NOTE 4 Des conséquences initiales peuvent déclencher des réactions en chaîne.

2.16
mesure de sécurité
moyens de gestion des **risques** (2.61), comprenant les **politiques** (2.51), les **procédures** (2.53), les **lignes directrices** (2.26), les pratiques ou l'organisation, qui peuvent être de nature administrative, technique, managériale ou juridique

NOTE 1 Dans le domaine de la sécurité de l'information, les mesures de sécurité comprennent tous les processus, politiques, procédures, lignes directrices, pratiques ou organisations, qui peuvent être de nature administrative, technique, managériale ou juridique, qui modifient les risques liés à la sécurité de l'information.

NOTE 2 Une mesure de sécurité peut ne pas aboutir à la modification voulue ou supposée.

NOTE 3 Mesure de sécurité est également synonyme de protection ou de contre-mesure.

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
action corrective
action visant à éliminer la cause d'une **non-conformité** (2.48) ou d'une autre situation indésirable détectée

[ISO 9000:2005]

2.19
données
ensemble des valeurs attribuées aux **mesures élémentaires** (2.11), aux **mesures dérivées** (2.21) et/ou aux **indicateurs** (2.27)

[ISO/CEI 15939:2007]

NOTE Cette définition s'applique uniquement dans le contexte de l'ISO/CEI 27004:2009.

2.20
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

[ISO/CEI 15939:2007]

2.21
mesure dérivée
mesure (2.43) définie en fonction d'au moins deux **mesures élémentaires** (2.11)

[ISO/CEI 15939:2007]

2.22
efficacité
niveau de réalisation des activités planifiées et d'obtention des résultats escomptés

[ISO 9000:2005]

2.23
efficience
rapport entre le résultat obtenu et les ressources utilisées

[ISO 9000:2005]

2.24
événement
occurrence ou changement d'un ensemble particulier de circonstances

[Guide ISO 73:2009]

NOTE 1 Un événement peut être unique ou se reproduire et peut avoir plusieurs causes.

NOTE 2 Un événement peut consister en quelque chose qui ne se produit pas.

NOTE 3 Un événement peut parfois être qualifié « d'incident » ou « d'accident ».

2.25
contexte externe
environnement externe dans lequel l'organisation cherche à atteindre ses objectifs

[Guide ISO 73:2009]

NOTE 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 de l'organisation, et
- les relations avec les parties prenantes externes, leurs perceptions et leurs valeurs.

2.26
ligne directrice
description clarifiant ce qu'il convient de réaliser et par quels moyens, en vue d'atteindre les objectifs fixés par la **politique** (2.51) de l'organisation

2.27
indicateur
mesure (2.43) qui fournit une estimation ou une évaluation d'**attributs** (2.6) spécifiés à partir d'un **modèle analytique** (2.3) concernant des **besoins d'information** (2.28) définis

2.28
besoin d'information
information nécessaire pour gérer les objectifs, les risques et les problèmes

[ISO/CEI 15939:2007]

2.29
moyens de traitement de l'information
tout système, service ou infrastructure de traitement de l'information, ou locaux les abritant

2.30
sécurité de l'information
protection de la **confidentialité** (2.13), de l'**intégrité** (2.36) et de la **disponibilité** (2.10) de l'information

NOTE En outre, d'autres propriétés, telles que l'**authenticité** (2.9), l'**imputabilité** (2.2), la **non-répudiation** (2.49) et la **fiabilité** (2.56), peuvent également être concernées.

2.31
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 protections ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité

2.32
incident lié à la sécurité de l'information
un ou plusieurs **événements liés à la sécurité de l'information** (2.31) 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** (2.30)

2.33
gestion des incidents liés à la sécurité de l'information
processus (2.54) pour détecter, rapporter, apprécier, intervenir, résoudre et tirer les enseignements des **incidents liés à la sécurité de l'information** (2.32)

2.34
système de management de la sécurité de l'information
SMSI
partie du **système de management** global (2.42), 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** (2.30)

NOTE Le système de management inclut l'organisation, les politiques, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources.

2.35
système d'information
application, service, actif informationnel ou toute autre composante permettant la prise en charge de l'information

2.36
intégrité
propriété de protection de l'exactitude et de la complétude des **actifs** (2.4)

2.37
contexte interne
environnement interne dans lequel l'organisation cherche à atteindre ses objectifs

[Guide ISO 73:2009]

NOTE Le contexte interne peut inclure :

- la gouvernance, l'organisation, 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, leurs perceptions et leurs valeurs,
- la culture de l'organisation,
- les normes, lignes directrices et modèles adoptés par l'organisation, et
- la forme et l'étendue des relations contractuelles.

2.38
projet SMSI
activités structurées entreprises par une organisation pour déployer un **SMSI** (2.34)

2.39
niveau de risque
importance d'un **risque** (2.61) exprimée en termes de combinaison des **conséquences** (2.15) et de leur **vraisemblance** (2.40)

[Guide ISO 73:2009]

2.40
vraisemblance
possibilité que quelque chose se produise

[Guide ISO 73:2009]

2.41
management
activités coordonnées visant à diriger et contrôler une organisation

[ISO 9000:2005]

2.42
système de management
cadre de référence des **lignes directrices** (2.26), **politiques** (2.51), **procédures** (2.53), **processus** (2.54) et ressources associées visant à assurer la réalisation des objectifs d'une organisation

2.43
mesure
variable à laquelle on attribue une valeur correspondant au résultat du **mesurage** (2.44)

[ISO/CEI 15939:2007]