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/IEC 2018



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2018

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en oeuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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 ... **iv**

Introduction ... **v**

1 Domaine d'application ... **1**

2 Références normatives ... **1**

3 Termes et definitions ... **1**

4 Systèmes de management de la sécurité de l'information ... **11**
4.1 Généralités ... 11
4.2 Qu'est-ce qu'un SMSI? ... 12
4.2.1 Vue d'ensemble et principes ... 12
4.2.2 L'information ... 13
4.2.3 Sécurité de l'information ... 13
4.2.4 Management ... 13
4.2.5 Système de management ... 13
4.3 Approche processus ... 14
4.4 Raisons expliquant pourquoi un SMSI est important ... 14
4.5 Établissement, surveillance, maintenance et amélioration d'un SMSI ... 15
4.5.1 Vue d'ensemble ... 15
4.5.2 Identifier les exigences liées à la sécurité de l'information ... 15
4.5.3 Apprécier les risques liés à la sécurité de l'information ... 16
4.5.4 Traiter les risques liés à la sécurité de l'information ... 16
4.5.5 Sélectionner et mettre en œuvre les mesures de sécurité ... 16
4.5.6 Surveiller, mettre à jour et améliorer l'efficacité du SMSI ... 17
4.5.7 Amélioration continue ... 18
4.6 Facteurs critiques de succès du SMSI ... 18
4.7 Avantages de la famille de normes du SMSI ... 19

5 La famille de normes du SMSI ... **19**
5.1 Informations générales ... 19
5.2 Norme donnant une vue d'ensemble et décrivant la terminologie ISO/IEC 27000 (le présent document) ... 20
5.3 Normes spécifiant des exigences ... 20
5.3.1 ISO/IEC 27001 ... 20
5.3.2 ISO/IEC 27006 ... 21
5.3.3 ISO/IEC 27009 ... 21
5.4 Normes décrivant des lignes directrices générales ... 21
5.4.1 ISO/IEC 27002 ... 21
5.4.2 ISO/IEC 27003 ... 22
5.4.3 ISO/IEC 27004 ... 22
5.4.4 ISO/IEC 27005 ... 22
5.4.5 ISO/IEC 27007 ... 22
5.4.6 ISO/IEC TR 27008 ... 23
5.4.7 ISO/IEC 27013 ... 23
5.4.8 ISO/IEC 27014 ... 23
5.4.9 ISO/IEC TR 27016 ... 24
5.4.10 ISO/IEC 27021 ... 24
5.5 Normes décrivant des lignes directrices propres à un secteur ... 24
5.5.1 ISO/IEC 27010 ... 24
5.5.2 ISO/IEC 27011 ... 25
5.5.3 ISO/IEC 27017 ... 25
5.5.4 ISO/IEC 27018 ... 25
5.5.5 ISO/IEC 27019 ... 26
5.5.6 ISO 27799 ... 27

Bibliographie ... **28**

© ISO/IEC 2018 – Tous droits réservés

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.

 © ISO/IEC 2018 – Tous droits réservés

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.

© ISO/IEC 2018 – Tous droits réservés

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.

© ISO 2018 – Tous droits réservés

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)

© ISO/IEC 2018 – Tous droits réservés

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.]

© ISO/IEC 2018 – Tous droits réservés

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

© ISO/IEC 2018 – Tous droits réservés

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]

© ISO/IEC 2018 – Tous droits réservés

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.]

© ISO/IEC 2018 – Tous droits réservés

3.46
surveillance
détermination du statut d'un système, d'un *processus* (3.54) 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.

3.47
non-conformité
non-satisfaction d'une *exigence* (3.56)

3.48
non-répudiation
capacité à prouver l'occurrence d'un *événement* (3.21) ou d'une action donnée(e) et des entités qui en sont à l'origine

3.49
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 concerner différentes disciplines (par exemple: finance, santé, sécurité ou environnement) et 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* (3.54).

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 définis par l'organisme, conformément à la politique de sécurité de l'information, afin d'obtenir des résultats spécifiques.

3.50
organisme
personne ou groupe de personnes qui exerce ses propres fonctions associées aux responsabilités, pouvoirs et relations nécessaires pour atteindre ses *objectifs* (3.49)

Note 1 à l'article: Le concept d'organisme inclut, sans s'y limiter, les travailleurs indépendants, compagnies, sociétés, firmes, entreprises, autorités, partenariats, œuvres de bienfaisance ou institutions, ou toute partie ou combinaison de ceux-ci, constituée en société de capitaux ou ayant un autre statut, de droit privé ou public.

3.51
externaliser
prendre des dispositions pour qu'un *organisme* (3.50) externe prenne en charge une partie des fonctions ou des *processus* (3.54) d'un organisme

Note 1 à l'article: Un organisme externe se situe hors du domaine d'application du *système de management* (3.41), mais les fonctions ou processus externalisés entrent dans le cadre de celui-ci.

3.52
performance
résultat mesurable

Note 1 à l'article: La performance peut se rapporter à des observations quantitatives ou qualitatives.

Note 2 à l'article: La performance peut se rapporter au management des activités, des *processus* (3.54), des produits (y compris les services), des systèmes ou des *organismes* (3.50).

3.53
politique
intentions et orientation d'un *organisme* (3.50) telles que formalisées par sa *direction* (3.75)

© ISO/IEC 2018 – Tous droits réservés

3.54
processus
ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie

3.55
fiabilité
propriété relative à un comportement et à des résultats prévus et cohérents

3.56
exigence
besoin ou attente formulé, généralement implicite ou obligatoire

Note 1 à l'article: «Généralement implicite» signifie qu'il est habituel ou courant, pour l'organisme et les parties intéressées, que le besoin ou l'attente en question soit implicite.

Note 2 à l'article: Une exigence spécifiée est une exigence formulée, par exemple une information documentée.

3.57
risque résiduel
risque (3.61) subsistant après le *traitement du risque* (3.72)

Note 1 à l'article: Un risque résiduel peut inclure un risque non identifié.

Note 2 à l'article: Un risque résiduel peut également être appelé «risque conservé».

3.58
revue
activité entreprise afin de déterminer l'adaptation, l'adéquation et *l'efficacité* (3.20) de l'objet étudié pour atteindre les *objectifs* (3.49) établis

[SOURCE: Guide ISO 73:2009, 3.8.2.2, modifié — Suppression de la note 1 à l'article.]

3.59
objet de revue
élément spécifique soumis à la revue

3.60
objectif de revue
déclaration décrivant le résultat attendu d'une *revue* (3.59)

3.61
risque
effet de l'incertitude sur les objectifs (3.49)

Note 1 à l'article: Un effet est un écart, positif ou négatif, par rapport à une attente.

Note 2 à l'article: L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

Note 3 à l'article: Un risque est souvent caractérisé en référence à des «événements» potentiels (tels que définis dans le Guide ISO 73:2009, 3.5.1.3) et des «conséquences» potentielles (telles que définies dans le Guide ISO 73:2009, 3.6.1.3), ou à une combinaison des deux.

Note 4 à l'article: Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa «vraisemblance» (telle que définie dans le Guide ISO 73:2009, 3.6.1.1).

Note 5 à l'article: Dans le contexte des systèmes de management de la sécurité de l'information, les risques liés à la sécurité de l'information peuvent être exprimés comme l'effet de l'incertitude sur les objectifs de sécurité de l'information.

Note 6 à l'article: Le risque lié à la sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités d'un actif ou d'un groupe d'actifs informationnels et nuisent donc à un organisme.

© ISO/IEC 2018 – Tous droits réservés

3.62
acceptation du risque
décision argumentée en faveur de la prise d'un *risque* (3.61) particulier

Note 1 à l'article: L'acceptation du risque peut avoir lieu sans *traitement du risque* (3.72) ou lors du *processus* (3.54) de traitement du risque.

Note 2 à l'article: Les risques acceptés font l'objet d'une *surveillance* (3.46) et d'une *revue* (3.58).

[SOURCE: Guide ISO 73:2009, 3.7.1.6]

3.63
analyse du risque
processus (3.54) mis en œuvre pour comprendre la nature d'un *risque* (3.61) et pour déterminer le *niveau de risque* (3.39)

Note 1 à l'article: L'analyse du risque fournit la base de l'*évaluation du risque* (3.67) et des décisions relatives au *traitement du risque* (3.72).

Note 2 à l'article: L'analyse du risque inclut l'estimation du risque.

[SOURCE: Guide ISO 73:2009, 3.6.1]

3.64
appréciation du risque
ensemble du *processus* (3.54) d'*identification du risque* (3.68), d'*analyse du risque* (3.63) et d'*évaluation du risque* (3.67)

Note 1 à l'article: [SOURCE: Guide ISO 73:2009, 3.4.1]

3.65
communication et concertation relatives au risque
ensemble de *processus* (3.54) itératifs et continus mis en œuvre par un organisme afin de fournir, partager ou obtenir des informations et d'engager un dialogue avec les *parties prenantes* (3.37) en ce qui concerne la gestion du *risque* (3.61)

Note 1 à l'article: Ces informations peuvent concerner l'existence, la nature, la forme, la *vraisemblance* (3.41), l'importance, l'évaluation, l'acceptabilité et le traitement du risque.

Note 2 à l'article: La concertation est un processus de communication argumentée à double sens entre un *organisme* (3.50) et ses parties prenantes sur une question donnée avant de prendre une décision ou de déterminer une orientation concernant cette question. La concertation est:

— un *processus* dont l'effet sur une décision s'exerce par l'influence plutôt que par le pouvoir, et

— une contribution à une prise de décision, et non une prise de décision conjointe.

3.66
critères de risque
termes de référence vis-à-vis desquels l'importance d'un *risque* (3.61) est évaluée

Note 1 à l'article: Les critères de risque sont fondés sur les objectifs de l'organisme et sur le *contexte externe* (3.22) et le *contexte interne* (3.38).

Note 2 à l'article: Les critères de risque peuvent être issus de normes, de lois, de *politiques* (3.53) et d'autres *exigences* (3.56).

[SOURCE: Guide ISO 73:2009, 3.3.1.3]

© ISO/IEC 2018 – Tous droits réservés

3.67
évaluation du risque
processus (3.54) de comparaison des résultats de l'*analyse du risque* (3.63) avec les *critères du risque* (3.66) afin de déterminer si le *risque* (3.61) et/ou son importance sont acceptables ou tolérables

Note 1 à l'article: L'évaluation du risque aide à la prise de décision relative au *traitement du risque* (3.72).

[SOURCE: Guide ISO 73:2009, 3.7.1]

3.68
identification des risques
processus (3.54) de recherche, de reconnaissance et de description des *risques* (3.61)

Note 1 à l'article: L'identification du risque comprend l'identification des sources de risque, des *événements* (3.21), de leurs causes et de leurs *conséquences* (3.12) potentielles.

Note 2 à l'article: L'identification du risque peut faire appel à des données historiques, des analyses théoriques et des avis d'experts et autres personnes compétentes, et tenir compte des besoins (3.37) des *parties prenantes*.

[SOURCE: Guide ISO 73:2009, 3.5.1]

3.69
gestion des risques
activités coordonnées visant à diriger et contrôler un *organisme* (3.50) vis-à-vis du *risque* (3.61)

[SOURCE: Guide ISO 73:2009, 2.1]

3.70
processus de management du risque
application systématique de *politiques* (3.53), procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de surveillance et de revue des *risques* (3.61)

Note 1 à l'article: L'ISO/IEC 27005 emploie le terme «*processus*» (3.54) pour décrire le management du risque dans sa globalité. Les éléments qui composent le processus de *management du risque* (3.69) sont appelés «activités».

[SOURCE: Guide ISO 73:2009, 3.1, modifié — Ajout de la note 1 à l'article.]

3.71
propriétaire du risque
personne ou entité ayant la responsabilité du *risque* (3.61) et ayant autorité pour le gérer

[SOURCE: Guide ISO 73:2009, 3.5.1.5]

3.72
traitement du risque
processus (3.54) destiné à modifier un *risque* (3.61)

Note 1 à l'article: Le traitement du risque peut inclure:

— un refus du risque en décidant de ne pas démarrer ni poursuivre l'activité porteuse du risque;

— la prise ou l'augmentation d'un risque afin de saisir une opportunité;

— l'élimination de la source de risque;

— une modification de la *vraisemblance* (3.40);

— une modification des *conséquences* (3.12);

— un partage du risque avec une ou plusieurs autres parties (incluant des contrats et un financement du risque);

— un maintien du risque fondé sur un choix argumenté.

© ISO/IEC 2018 – Tous droits réservés

Note 2 à l'article: Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque».

Note 3 à l'article: Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

[SOURCE: Guide ISO 73:2009, 3.8.1, modifié — «décision» a été remplacé par «choix» dans la note 1 à l'article.]

3.73
norme relative à la mise en œuvre de la sécurité
document qui spécifie les méthodes de mise en œuvre de la sécurité

3.74
menace
cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un *organisme* (3.50)

3.75
direction
personne ou groupe de personnes qui dirige et contrôle un *organisme* (3.50) au plus haut niveau

Note 1 à l'article: La direction a le pouvoir de déléguer l'autorité et de fournir des ressources au sein de l'organisme.

Note 2 à l'article: Si le domaine du *système de management* (3.41) ne s'étend qu'à une partie de l'organisme, la direction en réfère à l'équipe qui dirige et contrôle cette partie de l'organisme.

Note 3 à l'article: La direction est parfois appelée le management exécutif. Elle peut comprendre les présidents directeurs généraux, les directeurs financiers, les directeurs des systèmes d'information et autres fonctions similaires.

3.76
entité de communication des informations sécurisée
organisme (3.50) indépendant qui prend en charge l'échange d'informations dans une *communauté de partage d'informations* (3.34)

3.77
vulnérabilité
faille dans un actif ou dans une *mesure de sécurité* (3.14) qui peut être exploitée par une ou plusieurs *menaces* (3.74)

4 Systèmes de management de la sécurité de l'information

4.1 Généralités

Des organismes de toutes catégories et de toutes tailles:

a) collectent, traitent, stockent et transmettent des informations;

b) reconnaissent que les informations et les processus, systèmes, réseaux et personnes associés sont des actifs importants pour l'atteinte des objectifs de l'organisme;

c) font face à divers types de risques qui peuvent avoir des répercussions sur le fonctionnement des actifs; et

d) traitent l'exposition aux risques perçue en mettant en œuvre des mesures de sécurité de l'information.

Toutes les informations détenues et traitées par un organisme sont exposées à des menaces telles que des attaques, des erreurs, des événements naturels (une inondation ou un incendie, par exemple), etc., et sont exposées à des vulnérabilités inhérentes à leur utilisation. Le terme sécurité de l'information repose, en général, sur le fait que l'information est considérée comme un actif qui est doté d'une valeur

© ISO/IEC 2018 – Tous droits réservés