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)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

Les procédures utilisées pour élaborer le présent document et celles destinées à sa mise à jour sont décrites dans les Directives ISO/IEC, Partie 1. Il convient, en particulier de prendre note des différents critères d'approbation requis pour les différents types de documents ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets).

Les appellations commerciales éventuellement mentionnées dans le présent document sont données pour information, par souci de commodité, à l'intention des utilisateurs et ne sauraient constituer un engagement.

Pour une explication de la nature volontaire des normes, la signification des termes et expressions spécifiques de l'ISO liés à l'évaluation de la conformité, ou pour toute information au sujet de l'adhésion de l'ISO aux principes de l'Organisation mondiale du commerce (OMC) concernant les obstacles techniques au commerce (OTC), voir le lien suivant: www.iso.org/avant-propos.

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

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

— modification du texte de l'Introduction;

— suppression de certains termes et définitions;

— alignement de l'Article 3 par rapport à la structure-cadre pour MSS;

— mise à jour de l'Article 5 pour refléter les modifications dans les normes concernées;

— suppression des Annexes A et B.

Introduction

0.1 Vue d'ensemble

Les Normes internationales relatives aux systèmes de management fournissent un modèle en matière d'établissement et d'exploitation d'un système de management. Ce modèle comprend les caractéristiques que les experts dans le domaine s'accordent à reconnaître comme reflétant l'état de l'art au niveau international. Le sous-comité ISO/IEC JTC 1/SC 27 bénéficie de l'expérience d'un comité d'experts qui se consacre à l'élaboration des Normes internationales sur les systèmes de management pour la sécurité de l'information, connues également comme famille de normes du Système de Management de la Sécurité de l'Information (SMSI).

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

0.2 Objet du présent document

La famille de normes du SMSI comporte des normes qui:

a) définissent les exigences relatives à un SMSI et à ceux qui certifient de tels systèmes;

b) apportent des informations directes, des recommandations et/ou une interprétation détaillées concernant le processus général visant à établir, mettre en œuvre, maintenir et améliorer un SMSI;

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

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

0.3 Contenu du présent document

Dans le présent document, les formes verbales suivantes sont utilisées:

— «doit» indique une exigence;

— «il convient» indique une recommandation;

— «peut» indique une autorisation («may» en anglais),

— ou une possibilité ou une capacité («can» en anglais).

Les informations sous forme de «NOTE» sont fournies pour clarifier l'exigence associée ou en faciliter la compréhension. Les «Notes à l'article» employées à l'Article 3 fournissent des informations supplémentaires qui viennent compléter les données terminologiques et peuvent contenir des dispositions concernant l'usage d'un terme.

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

1 Domaine d'application

Le présent document offre une vue d'ensemble des systèmes de management de la sécurité de l'information (SMSI). Il comprend également les termes et définitions d'usage courant dans la famille de normes du SMSI. Le présent document est applicable à tous les types et à toutes les tailles d'organismes (par exemple: les entreprises commerciales, les organismes publics, les organismes à but non lucratif).

Les termes et les définitions fournis dans le présent document:

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

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

— ne limitent pas la famille de normes du SMSI en définissant de nouveaux termes à utiliser.

2 Références normatives

Le présent document ne contient aucune référence normative.

3 Termes et definitions

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse http://www.electropedia.org/

3.1
contrôle d'accès
moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les *exigences* (3.56) propres à la sécurité et à l'activité métier

3.2
attaque
tentative de détruire, de rendre public, de modifier, d'invalider, de voler ou d'utiliser sans autorisation un actif, ou de faire un usage non autorisé de celui-ci

3.3
audit
processus méthodique, indépendant et documenté (3.54) permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits

Note 1 à l'article: Un audit peut être interne (audit de première partie), externe (audit de seconde ou de tierce partie) ou combiné (associant deux disciplines ou plus).

Note 2 à l'article: Un audit interne est réalisé par l'organisme lui-même ou par une partie externe pour le compte de celui-ci.

Note 3 à l'article: Les termes «preuves d'audit» et «critères d'audit» sont définis dans l'ISO 19011.

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

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

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

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

3.7
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée

3.8
mesure élémentaire
mesure (3.42) définie en fonction d'un attribut et de la méthode de mesurage spécifiée pour le quantifier

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

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.3, modifiée — Suppression de la note 2 à l'article.]

3.9
compétence
capacité à appliquer des connaissances et des aptitudes pour obtenir les résultats escomptés

3.10
confidentialité
propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des *processus* (3.54) non autorisés

3.11
conformité
satisfaction d'une *exigence* (3.56)

3.12
conséquence
effet d'un *événement* (3.21) affectant les *objectifs* (3.49)

Note 1 à l'article: Un événement peut engendrer une série de conséquences.

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

Note 3 à l'article: Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Note 4 à l'article: Des conséquences initiales peuvent déclencher des réactions en chaîne.

[SOURCE: Guide ISO 73:2009, 3.6.1.3, modifié — Modification de la Note 2 à l'article après «et».]

3.13
amélioration continue
activité régulière destinée à améliorer les *performances* (3.52)

3.14
mesure de sécurité
mesure qui modifie un *risque* (3.61)

Note 1 à l'article: Les mesures de sécurité comprennent tous les *processus* (3.54), *politiques* (3.53), dispositifs, pratiques ou autres actions qui modifient un *risque* (3.61).

Note 2 à l'article: Il est possible que les mesures de sécurité ne puissent pas toujours aboutir à la modification voulue ou supposée.

[SOURCE: Guide ISO 73:2009, 3.8.1.1, — Modification de la Note 2 à l'article.]

3.15
objectif d'une mesure de sécurité
déclaration décrivant ce qui est attendu de la mise en œuvre des *mesures de sécurité* (3.14)

3.16
correction
action visant à éliminer une *non-conformité* (3.47) détectée

3.17
action corrective
action visant à éliminer la cause d'une *non-conformité* (3.47) et à empêcher qu'elle ne se répète

3.18
mesure dérivée
mesure (3.42) définie en fonction d'au moins deux *mesures élémentaires* (3.8)

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.8, modifiée — Suppression de la note 1 à l'article.]

3.19
informations documentées
informations devant être contrôlées et mises à jour par un *organisme* (3.50) et le support sur lequel elles sont stockées

Note 1 à l'article: Les informations documentées peuvent être dans n'importe quel format, sur n'importe quel support et provenir de n'importe quelle source.

Note 2 à l'article: Les informations documentées peuvent se rapporter:

— au *système de management* (3.41) et aux *processus* associés (3.54);

— aux informations créées pour permettre à l'*organisme* (3.50) de fonctionner (documentation);

— aux preuves des résultats obtenus (enregistrements).

3.20
efficacité
niveau de réalisation des activités planifiées et d'obtention des résultats escomptés

3.21
événement
occurrence ou changement d'un ensemble particulier de circonstances

Note 1 à l'article: Un événement peut être unique ou se reproduire. Il peut avoir plusieurs causes.

Note 2 à l'article: Un événement peut consister en quelque chose qui ne se produit pas.

Note 3 à l'article: Un événement peut parfois être qualifié «d'incident» ou «d'accident».

[SOURCE: Guide ISO 73:2009, 3.5.1.3, modifié — Suppression de la note 4 à l'article.]

3.22
contexte externe
environnement externe dans lequel l'organisme cherche à atteindre ses *objectifs* (3.49)

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

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

— *les facteurs clés et tendances ayant un impact déterminant sur les objectifs* de l'organisme (3.50);

— les relations avec les *parties prenantes* (3.37) externes, les perceptions et valeurs relatives à celles-ci.

[SOURCE: Guide ISO 73:2009, 3.3.1.1]

3.23
gouvernance de la sécurité de l'information
système par lequel un *organisme* (3.50) conduit et supervise les activités liées à la *sécurité de l'information* (3.28)

3.24
instances dirigeantes
personne ou groupe de personnes ayant la responsabilité des *performances* (3.52) et de la conformité de l'*organisme* (3.50)

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

3.25
indicateur
mesure (3.42) qui fournit une estimation ou une évaluation

3.26
besoin d'information
information nécessaire pour gérer les *objectifs* (3.49), les buts, les risques et les problèmes

[SOURCE: ISO/IEC/IEEE 15939:2017, 3.12]

3.27
moyens de traitement de l'information
tout système, service ou infrastructure de traitement de l'information, ou le local les abritant

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

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

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

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

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

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

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

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

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

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

3.36
intégrité
propriété d'exactitude et de complétude

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

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

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

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

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

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

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

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

— la culture de l'organisme;

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

— la forme et l'étendue des relations contractuelles.

[SOURCE: Guide ISO 73:2009, 3.3.1.2]

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

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

3.40
vraisemblance
possibilité que quelque chose se produise

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

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

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

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

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

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

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

3.43
mesurage
processus (3.54) permettant de déterminer une valeur

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

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

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

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

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

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

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

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)

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.

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]

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.

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

et qui doit bénéficier d'une protection appropriée contre la perte de disponibilité, de confidentialité et d'intégrité, par exemple. Garantir l'accès par les personnes qui y sont autorisées et qui en ont besoin à des informations exactes et complètes au moment où elles le souhaitent permet de contribuer à l'efficacité de l'entreprise.

Protéger les actifs informationnels en définissant, garantissant, maintenant et améliorant efficacement la sécurité de l'information est essentiel pour permettre à un organisme d'atteindre ses objectifs et de maintenir et améliorer ses obligations légales et son image. Ces activités coordonnées visant à orienter la mise en œuvre de mesures appropriées et à traiter les risques inacceptables liés à la sécurité de l'information, sont généralement connues comme étant des éléments de management de la sécurité de l'information.

Étant donné que les risques liés à la sécurité de l'information et l'efficacité des mesures évoluent en fonction de la conjoncture, les organismes doivent:

a) surveiller et évaluer l'efficacité des mesures de sécurité et des procédures mises en œuvre;

b) identifier les risques émergents à traiter; et

c) sélectionner, mettre en œuvre et améliorer les mesures de sécurité appropriées le cas échéant.

Pour relier ces activités de sécurité de l'information et les coordonner, chaque organisme doit établir sa politique et ses objectifs en matière de sécurité de l'information et utiliser un système de management lui permettant d'atteindre ces objectifs de manière efficace.

4.2 Qu'est-ce qu'un SMSI?

4.2.1 Vue d'ensemble et principes

Un SMSI se compose des politiques, procédures, lignes directrices et des ressources et activités associées, gérées collectivement par un organisme dans le but de protéger ses actifs informationnels. Un SMSI utilise une approche systématique visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, maintenir et améliorer la sécurité de l'information d'un organisme afin que celui-ci atteigne ses objectifs métier. Cette approche se fonde sur l'appréciation du risque et sur les niveaux d'acceptation du risque définis par l'organisme pour traiter et gérer efficacement les risques. L'analyse des exigences de protection des actifs informationnels et l'application des mesures appropriées pour assurer comme il se doit la protection de ces actifs, contribuent à la réussite de la mise en œuvre d'un SMSI. Les principes essentiels suivants y contribuent également:

a) la sensibilisation à la sécurité de l'information;

b) l'attribution des responsabilités liées à la sécurité de l'information;

b) la prise en compte de l'engagement de la direction et des intérêts des parties prenantes;

d) la consolidation des valeurs sociétales;

e) les appréciations du risque déterminant les mesures de sécurité appropriées pour arriver à des niveaux de risque acceptables;

f) l'intégration de la sécurité comme élément essentiel des systèmes et des réseaux d'information;

g) la prévention et la détection actives des incidents liés à la sécurité de l'information;

h) l'adoption d'une approche globale du management de la sécurité de l'information;

i) le réexamen continu de l'appréciation de la sécurité de l'information et la mise en œuvre de modifications le cas échéant.

4.2.2 L'information

L'information est un actif qui, comme tous les autres actifs importants de l'organisme, est essentiel à son fonctionnement et qui, par conséquent, requiert une protection adéquate. Elle peut être stockée sous différentes formes, notamment numérique (par exemple: des fichiers de données stockés sur un support électronique ou optique), matérielle (par exemple: sur papier) ou en tant qu'information intangible (par exemple: les connaissances des salariés). L'information peut être transmise par différents moyens, notamment par courrier ou dans le cadre de communications électroniques ou verbales. Quelle que soit la forme que prend l'information ou quel que soit son vecteur de transmission, elle requiert une protection appropriée.

Dans de nombreux organismes, l'information dépend des technologies de l'information et des communications. Ces technologies représentent souvent un élément essentiel dans l'organisme et elles facilitent la création, le traitement, le stockage, la transmission, la protection et la destruction de l'information.

4.2.3 Sécurité de l'information

La sécurité de l'information garantit la confidentialité, la disponibilité et l'intégrité de l'information. Afin de contribuer au succès de l'organisme et à sa pérennité, et de réduire le plus possible l'impact des incidents liés à la sécurité de l'information, la sécurité de l'information implique l'application et le management de mesures de sécurité appropriées, ce qui sous-entend la prise en compte d'un vaste éventail de menaces.

La sécurité de l'information s'obtient par la mise en œuvre d'un ensemble de mesures de sécurité applicables, sélectionnées au moyen d'un processus déterminé de management du risque et gérées à l'aide d'un SMSI contenant les politiques, processus, procédures, structures organisationnelles, logiciels et matériels permettant de protéger les actifs informationnels identifiés. Ces mesures doivent être spécifiées, mises en œuvre, surveillées, réexaminées et améliorées, si nécessaire, pour s'assurer qu'elles répondent aux objectifs métier et sécurité de l'information spécifiques de l'organisme. Il est attendu que les mesures de sécurité pertinentes de sécurité de l'information s'intègrent parfaitement aux processus métier de l'organisme.

4.2.4 Management

Le management implique des activités de pilotage, de contrôle et d'amélioration continue de l'organisme dans des structures appropriées. Les activités de management incluent les actions, la manière ou les pratiques instaurées pour organiser, prendre en charge, diriger, superviser et contrôler les ressources. Les structures de management peuvent aller d'une personne dans un petit organisme à des hiérarchies de management composées d'un grand nombre de personnes dans les grands organismes.

Au sens d'un SMSI, le management implique la supervision et la prise de décisions nécessaires à l'atteinte des objectifs métier par le biais de la protection des actifs informationnels de l'organisme. Le management de la sécurité de l'information s'exprime au travers de la formulation et de l'utilisation de politiques, de procédures et de lignes directrices relatives à la sécurité de l'information, qui sont ensuite appliquées à tous les niveaux de l'organisme par toutes les personnes qui y sont associées.

4.2.5 Système de management

Un système de management utilise un cadre de référence permettant à un organisme d'atteindre ses objectifs. Il comprend la structure organisationnelle, les politiques, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources.

En termes de sécurité de l'information, un système de management permet à un organisme:

a) de satisfaire aux exigences en matière de sécurité de l'information des clients et des autres parties prenantes;

b) d'améliorer les plans et les activités d'un organisme;

c) de répondre aux objectifs de sécurité de l'information de l'organisme;

d) de se conformer aux réglementations, à la législation et aux autorités sectorielles; et

e) de gérer les actifs informationnels d'une manière organisée qui facilite l'amélioration et l'ajustement continus aux objectifs actuels de l'organisme.

4.3 Approche processus

Pour fonctionner de manière efficace et efficiente, les organismes doivent identifier et gérer de nombreuses activités. Toute activité qui utilise des ressources doit être gérée pour permettre la transformation d'éléments d'entrée en éléments de sortie à l'aide d'un ensemble d'activités corrélées ou interactives. Ce type d'activité est également connu sous le nom de «processus». Les éléments de sortie d'un processus peuvent être utilisés en tant qu'éléments d'entrée d'un autre processus et, généralement, cette transformation s'opère dans des conditions planifiées et maîtrisées. L'«approche processus» peut désigner l'application d'un système de processus au sein d'un organisme, ainsi que l'identification, les interactions et le management de ces processus.

4.4 Raisons expliquant pourquoi un SMSI est important

Il est nécessaire de traiter les risques associés aux actifs informationnels d'un organisme. Mener à bien la sécurité de l'information requiert un management du risque et englobe les risques qui découlent des menaces physiques, humaines et technologiques associées aux informations sous toutes leurs formes, au sein de l'organisme ou utilisées par l'organisme.

Pour un organisme, l'adoption d'un SMSI est, en principe, une décision stratégique et il est nécessaire que cette décision soit intégrée sans heurts, dimensionnée et actualisée en fonction des besoins de l'organisme.

La conception et la mise en œuvre du SMSI d'un organisme sont influencées par les besoins et les objectifs de l'organisme, les exigences de sécurité, les processus mis en œuvre, ainsi que par la taille et la structure de l'organisme. La conception et la mise en œuvre d'un SMSI doivent correspondre aux intérêts et aux exigences en matière de sécurité de l'information de toutes les parties prenantes de l'organisme, y compris les clients, les fournisseurs, les partenaires commerciaux, les actionnaires et toutes les autres tierces parties concernées.

Dans un monde interconnecté, l'information et les processus, systèmes et réseaux qui s'y rapportent constituent des actifs critiques de l'organisme. Les organismes et leurs systèmes et réseaux d'informations sont confrontés à des menaces pour la sécurité dont les origines sont très variées: fraude assistée par ordinateur, espionnage, sabotage, vandalisme, incendies ou inondations, par exemple. Les dommages causés aux systèmes et aux réseaux d'information par des programmes malveillants, le piratage informatique et des attaques de type Refus de service sont de plus en plus courants, ambitieux et sophistiqués.

Le SMSI est important autant pour les activités du secteur public que pour celles du secteur privé. Dans toutes les branches d'activité, le SMSI est un instrument qui favorise le commerce électronique et qui s'avère essentiel aux activités de management du risque. L'interconnexion des réseaux publics et privés et le partage des actifs informationnels augmentent les difficultés liées au traitement de l'information et au contrôle de son accès. En outre, la distribution de dispositifs de stockage mobiles contenant des actifs informationnels peut affaiblir l'efficacité des mesures de sécurité traditionnelles. Quand des organismes adoptent la famille de normes du SMSI, il est possible de démontrer à leurs partenaires et aux autres parties intéressées que l'application de principes de sécurité de l'information cohérents et mutuellement reconnaissables est possible.

La sécurité de l'information n'est pas toujours prise en compte lors de la conception et de l'élaboration des systèmes d'information. En outre, elle est souvent envisagée comme une solution technique. Pourtant, la sécurité de l'information qui peut être assurée par des moyens techniques est limitée et elle peut s'avérer inefficace sans l'aide d'un management et de procédures appropriés définis dans le contexte d'un SMSI. L'intégration après coup de la sécurité à un système d'information opérationnel

peut s'avérer difficile et coûteuse. Un SMSI implique une identification des mesures de sécurité mises en place et exige une planification soignée et une grande attention portée aux détails. À titre d'exemple, les contrôles d'accès, qui peuvent être techniques (logiques), physiques, administratifs (managériaux) ou consister en une combinaison de ces différents types de contrôle, permettent de s'assurer que l'accès aux actifs informationnels est autorisé et limité conformément aux exigences liées à l'activité et à la sécurité de l'information.

L'adoption d'un SMSI est un élément important de la protection des actifs informationnels qui permet à un organisme:

a) de conforter son assurance concernant la protection correcte des actifs informationnels contre les menaces et la permanence de cette protection;

b) de maintenir un cadre de référence structuré et exhaustif visant à identifier et apprécier les risques liés à la sécurité de l'information, par le choix et la mise en œuvre des mesures de sécurité appropriées et par la mesure et l'amélioration de leur efficacité;

c) d'améliorer continuellement son environnement de contrôle; et

d) de remplir ses obligations légales et garantir sa conformité réglementaire de manière efficace.

4.5 Établissement, surveillance, maintenance et amélioration d'un SMSI

4.5.1 Vue d'ensemble

Un organisme doit suivre les étapes suivantes pour établir, surveiller, maintenir et améliorer son SMSI:

a) identifier les actifs informationnels et les exigences de sécurité de l'information associées (voir 4.5.2);

b) apprécier les risques liés à la sécurité de l'information (voir 4.5.3) et traiter les risques liés à la sécurité de l'information (voir 4.5.4);

c) sélectionner et mettre en œuvre les mesures de sécurité pertinentes pour gérer les risques inacceptables (voir 4.5.5);

d) surveiller, mettre à jour et améliorer l'efficacité des mesures de sécurité associées aux actifs informationnels de l'organisme (voir 4.5.6).

Pour s'assurer que le SMSI protège efficacement et sans interruption les actifs informationnels de l'organisme, il est nécessaire de répéter en boucle les étapes a) à d) afin d'identifier les changements qui affectent les risques, les stratégies de l'organisme ou ses objectifs métier.

4.5.2 Identifier les exigences liées à la sécurité de l'information

Dans le cadre de la stratégie globale et des objectifs métier de l'organisme, de sa taille et de son extension géographique, les exigences de sécurité de l'information peuvent être identifiées par la compréhension des éléments suivants:

a) les actifs informationnels identifiés et la valeur associée;

b) les besoins métier de l'organisme en traitement, stockage et communication de l'information;

c) les exigences légales, réglementaires et contractuelles.

Pour évaluer de manière méthodique les risques associés aux actifs informationnels de l'organisme, il est nécessaire d'analyser les menaces qui pèsent sur les actifs informationnels, les vulnérabilités à une menace sur les actifs informationnels et la vraisemblance d'une telle menace, ainsi que l'impact potentiel d'un éventuel incident lié à la sécurité de l'information sur les actifs informationnels. Les dépenses consacrées aux mesures de sécurité pertinentes doivent, en principe, être proportionnelles à l'impact de la concrétisation du risque tel qu'il est perçu par l'organisme.

4.5.3 Apprécier les risques liés à la sécurité de l'information

La gestion des risques liés à la sécurité de l'information exige une méthode correcte d'appréciation et de traitement du risque qui peut inclure une estimation des coûts et des bénéfices, des exigences légales, des préoccupations des parties prenantes et d'autres données et variables, si nécessaire.

Il convient que l'appréciation du risque identifie, quantifie et hiérarchise les risques par rapport à des critères d'acceptation du risque et à des objectifs pertinents pour l'organisme. Il convient que les résultats ainsi obtenus guident la direction dans son action et dans l'établissement de ses priorités en matière de management des risques liés à la sécurité de l'information et de mise en œuvre des mesures de sécurité sélectionnées pour assurer une protection contre ces risques.

Il convient que l'appréciation du risque intègre:

— l'approche systématique consistant à estimer l'importance des risques (analyse du risque) et

— le processus consistant à comparer les risques estimés à des critères de risque afin de déterminer l'importance des risques (évaluation du risque).

Il convient de réaliser périodiquement l'appréciation du risque afin de tenir compte de l'évolution des exigences en matière de sécurité de l'information et de l'évolution de la situation du risque (par exemple: au niveau des actifs, des menaces, des vulnérabilités, des impacts, de l'évaluation du risque), et à chaque changement important. Il convient de mettre en œuvre ces appréciations du risque en procédant d'une manière méthodique qui permette de produire des résultats comparables et reproductibles.

Pour être efficace, il convient de définir clairement l'étendue de l'appréciation du risque lié à la sécurité de l'information et d'y inclure des relations avec des appréciations du risque portant sur d'autres points, le cas échéant.

L'ISO/IEC 27005 contient des recommandations relatives au management du risque lié à la sécurité de l'information et des conseils sur l'appréciation, le traitement, l'acceptation, la surveillance, la revue du risque et la création de rapports concernant celui-ci. Elle donne également des exemples de méthodologies d'appréciation du risque.

4.5.4 Traiter les risques liés à la sécurité de l'information

Avant d'envisager le traitement d'un risque, il convient que l'organisme définisse des critères afin de déterminer si tel ou tel risque peut être accepté. Un risque peut être accepté, par exemple, si l'on estime qu'il est faible ou que son traitement ne sera pas rentable pour l'organisme. Il convient de consigner ces décisions.

Suite à l'appréciation des risques, il est nécessaire de prendre une décision concernant le traitement de chacun des risques identifiés. Voici quelques exemples d'options possibles en matière de traitement du risque:

a) l'application de mesures de sécurité appropriées pour réduire les risques;

b) l'acceptation délibérée et objective des risques, à condition qu'ils satisfassent clairement à la politique et aux critères définis par l'organisme en matière d'acceptation du risque;

c) le refus des risques par l'interdiction des actions susceptibles de les provoquer;

d) le partage des risques associés avec d'autres parties (par exemple: les assureurs ou les fournisseurs).

Pour les risques qu'il a été décidé de traiter par l'application de mesures de sécurité appropriées, il convient de sélectionner et de mettre en œuvre ces mesures de sécurité.

4.5.5 Sélectionner et mettre en œuvre les mesures de sécurité

Une fois que les exigences de sécurité de l'information ont été identifiées (voir 4.5.2), que les risques liés à la sécurité des actifs informationnels identifiés ont été déterminés et appréciés (voir 4.5.3) et que

les décisions concernant le traitement des risques liés à la sécurité de l'information ont été prises (voir 4.5.4), la sélection et la mise en œuvre des mesures de sécurité appropriées pour réduire les risques s'appliquent.

Il convient que ces mesures de sécurité permettent de ramener les risques à un seuil acceptable en prenant en compte:

a) les exigences et les contraintes de la législation et des réglementations nationales et internationales;

b) les objectifs de l'organisme;

c) les exigences et les contraintes d'exploitation;

d) le coût de mise en œuvre et d'exploitation par rapport à la réduction effective des risques, et proportionnellement aux exigences et aux contraintes de l'organisme;

e) leurs objectifs en matière de mise en œuvre, de surveillance et d'amélioration de l'efficience et l'efficacité des mesures de sécurité de l'information afin de soutenir les objectifs de l'organisme. Pour mieux répondre aux exigences de conformité, il convient de documenter la sélection et la mise en œuvre des mesures de sécurité dans une déclaration d'applicabilité;

f) la nécessité d'équilibrer l'investissement consenti pour la mise en œuvre et l'exploitation des mesures de sécurité, au regard des pertes susceptibles d'être occasionnées par des incidents liés à la sécurité de l'information.

Les mesures de sécurité spécifiées dans l'ISO/IEC 27002 sont reconnus comme de bonnes pratiques applicables à la plupart des organismes et facilement adaptables aux diverses envergures et complexités des organismes. D'autres normes de la famille de normes du SMSI fournissent des recommandations sur la sélection et l'application des mesures de sécurité de l'ISO/IEC 27002 pour le SMSI.

Il convient d'envisager les mesures de sécurité de l'information au stade de conception et de spécification des exigences relatives aux systèmes et aux projets. Tout manquement à cette recommandation peut engendrer des coûts supplémentaires et conduire à des solutions moins efficaces voire, dans le pire des cas, à une incapacité à assurer la sécurité adéquate. Les mesures de sécurité peuvent être sélectionnées dans l'ISO/IEC 27002 ou dans d'autres ensembles de mesures de sécurité. Sinon, de nouvelles mesures de sécurité correspondant aux besoins spécifiques de l'organisme peuvent également être définies. Il est nécessaire de reconnaître qu'il est possible que certaines mesures de sécurité ne soient pas applicables à tous les systèmes d'information ni à tous les environnements, et qu'elles ne soient pas réalisables pour tous les organismes.

La mise en œuvre d'un ensemble de mesures de sécurité choisi prend parfois du temps et, pendant cette période, le niveau de risque peut être plus élevé que ce qui est tolérable à long terme. Il convient que les critères de risque couvrent la tolérabilité des risques à court terme, le temps de mettre en œuvre les mesures de sécurité. Il convient que les parties intéressées soient tenues régulièrement informées des niveaux de risque estimés ou attendus pendant la mise en œuvre progressive des mesures de sécurité.

Il convient de garder à l'esprit qu'aucun ensemble de mesures de sécurité ne peut assurer la sécurité complète de l'information. Il convient que la direction mette en œuvre d'autres actions afin de surveiller, d'évaluer et d'améliorer l'efficience et l'efficacité des mesures de sécurité de l'information, pour soutenir les objectifs de l'organisme.

Pour mieux répondre aux exigences de conformité, il convient de documenter la sélection et la mise en œuvre des mesures de sécurité dans une déclaration d'applicabilité.

4.5.6 Surveiller, mettre à jour et améliorer l'efficacité du SMSI

Tout organisme doit maintenir et améliorer son SMSI en surveillant et appréciant ses performances par rapport à ses politiques et à ses objectifs, ainsi qu'en soumettant ses résultats à la direction à des fins de vérification. Cette procédure permet de contrôler que le SMSI contient des mesures de sécurité spécifiées permettant de traiter les risques appartenant au domaine d'application du SMSI. En outre, elle

permet d'apporter la preuve de la vérification et de la traçabilité des actions correctives, préventives et d'amélioration en se fondant sur les enregistrements de ces points de surveillance.

4.5.7 Amélioration continue

Le but de l'amélioration continue d'un SMSI est d'augmenter la probabilité de réaliser des objectifs en matière de préservation de la confidentialité, de disponibilité et d'intégrité de l'information. L'amélioration continue est centrée sur la recherche de possibilités d'amélioration, sans partir du principe que les activités de management existantes sont suffisantes, ou aussi appropriées que possible.

Voici quelques exemples de ces actions:

a) l'analyse et l'évaluation de la situation existante pour identifier des domaines d'amélioration;

b) l'établissement des objectifs d'amélioration;

c) la recherche de solutions possibles pour atteindre ces objectifs;

d) l'évaluation de ces solutions et la réalisation d'une sélection;

e) la mise en œuvre de la solution choisie;

f) le mesurage, la vérification, l'analyse et l'évaluation des résultats de la mise en œuvre pour déterminer si les objectifs ont été atteints;

g) l'officialisation des modifications.

Si nécessaire, les résultats sont étudiés afin d'identifier d'autres opportunités d'amélioration. Dans cette optique, l'amélioration est une activité continue, ce qui signifie que les actions sont répétées fréquemment. Les retours d'information des clients et des autres parties intéressées, les audits et la revue du système de management de la sécurité de l'information peuvent également être utilisés pour identifier des opportunités d'amélioration.

4.6 Facteurs critiques de succès du SMSI

De nombreux facteurs sont essentiels pour réussir la mise en œuvre d'un SMSI permettant à un organisme de répondre à ses objectifs métier. Voici quelques exemples de facteurs critiques de succès:

a) une politique, des objectifs et des activités de sécurité de l'information en phase avec les objectifs de l'organisme;

b) une approche et un cadre pour la conception, la mise en œuvre, la surveillance, le maintien et l'amélioration de la sécurité de l'information, cohérents avec la culture de l'organisme;

c) une adhésion et un engagement visibles à tous les niveaux du management, notamment au niveau de la direction;

d) une compréhension des exigences de protection des actifs informationnels via l'application de mesures de management du risque lié à la sécurité de l'information (voir ISO/IEC 27005);

e) un programme efficace de sensibilisation, de formation et d'éducation à la sécurité de l'information, qui informe tous les salariés et autres parties concernées de leurs obligations en matière de sécurité de l'information, telles qu'elles sont détaillées dans les politiques, normes, etc. en matière de sécurité de l'information, et qui les motive à agir en conséquence;

f) un processus efficace de gestion des incidents liés à la sécurité de l'information;

g) une approche efficace de management de la continuité de l'activité;

h) un système de mesurage utilisé pour évaluer la performance du management de la sécurité de l'information et des suggestions d'amélioration issues des retours d'information.

Un SMSI augmente la probabilité de voir un organisme réunir de façon cohérente les facteurs critiques de succès nécessaires à la protection de ses actifs informationnels.

4.7 Avantages de la famille de normes du SMSI

Les avantages de la mise en œuvre d'un SMSI découlent principalement d'une réduction des risques liés à la sécurité de l'information (à savoir la réduction de la probabilité et/ou de l'impact des incidents liés à la sécurité de l'information). Plus précisément, les avantages proposés pour permettre à un organisme de bénéficier d'une réussite durable suite à l'adoption de la famille de normes du SMSI comprennent:

a) une méthode structurée soutenant le processus de définition, de mise en œuvre, d'exploitation et de maintenance d'un SMSI intégré et aligné, à valeur ajoutée, exhaustif et rentable, qui réponde aux besoins de l'organisme sur différents sites et modes de fonctionnement;

b) une aide à la direction permettant de gérer et d'exploiter de façon cohérente et responsable l'approche du management de la sécurité de l'information, dans le contexte de gouvernance et de management des risques de l'entreprise, comprenant des actions d'éducation et de formation sur le management global de la sécurité de l'information, destinées aux responsables métier et propriétaires système;

c) la promotion de bonnes pratiques de sécurité de l'information admises dans le monde entier, de façon non dogmatique, qui donnent aux organismes la latitude nécessaire pour adopter et améliorer les mesures de sécurité appropriées qui conviennent à leurs situations spécifiques et pour les mettre à jour face aux changements internes et externes;

d) la mise à disposition d'un langage et de fondements conceptuels communs de sécurité de l'information, qui favorisent la confiance envers les partenaires commerciaux qui possèdent un SMSI conforme, en particulier s'ils sollicitent la certification selon l'ISO/IEC 27001 auprès d'un organisme de certification accrédité;

e) le renforcement de la confiance accordée à l'organisme par les parties prenantes;

f) la satisfaction des attentes et des besoins sociétaux;

g) une gestion économique plus efficace des investissements dans le domaine de la sécurité de l'information.

5 La famille de normes du SMSI

5.1 Informations générales

La famille de normes du SMSI se compose de normes interdépendantes, déjà publiées ou en cours d'élaboration, et comporte un certain nombre de composantes structurelles importantes. Ces composantes s'articulent autour de:

— normes qui décrivent les exigences du SMSI (ISO/IEC 27001);

— les exigences des organismes de certification (ISO/IEC 27006) pour les entités en charge de la certification de la conformité à l'ISO/IEC 27001;

— le cadre des exigences supplémentaires pour les mises en œuvre du SMSI propres à des secteurs particuliers (ISO/IEC 27009).

D'autres documents fournissent des recommandations sur divers aspects de la mise en œuvre d'un SMSI, avec un processus générique ainsi que des recommandations spécifiques à un secteur.

Les relations au sein de la famille de normes du SMSI sont illustrées à la Figure 1.

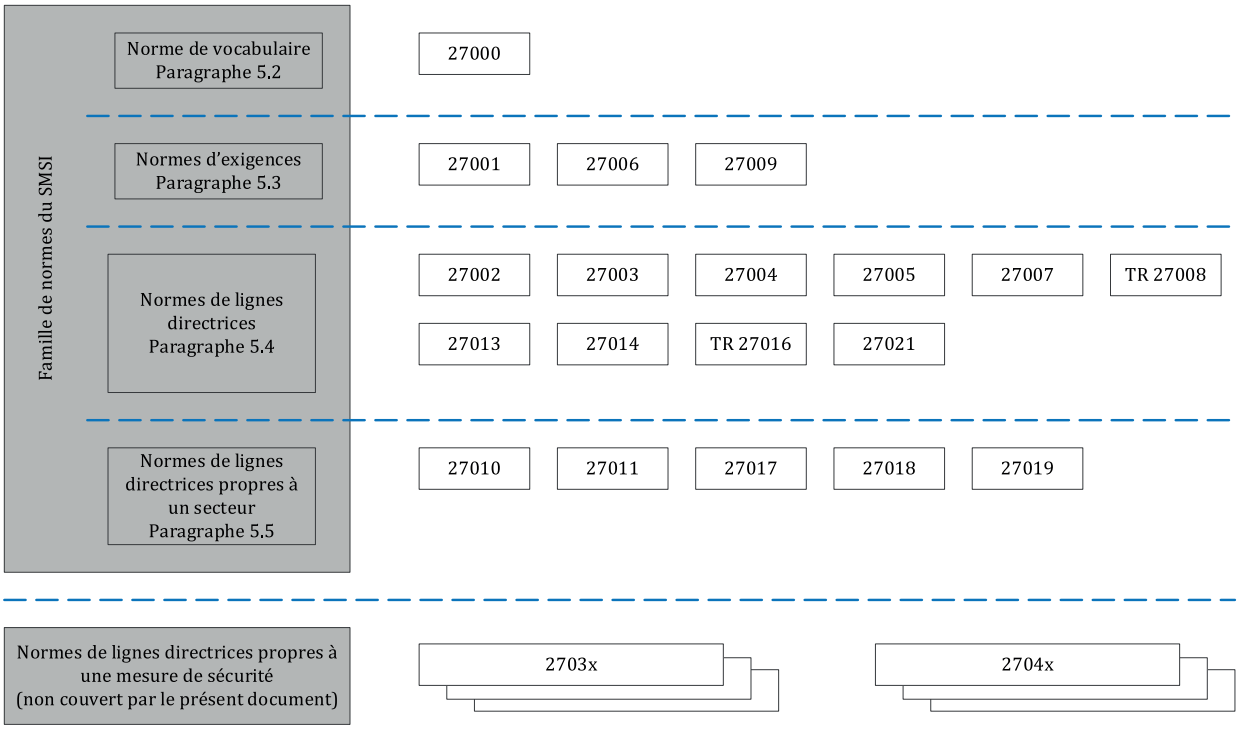

Figure 1 — Relations au sein de la famille de normes du SMSI

Chacune des normes de la famille du SMSI est décrite ci-dessous d'après son type (ou son rôle) au sein de la famille de normes du SMSI et d'après son numéro de référence.

5.2 Norme donnant une vue d'ensemble et décrivant la terminologie ISO/IEC 27000 (le présent document)

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

Domaine d'application: Le présent document fournit aux organismes et aux personnes:

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; et

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

Objectif: Le présent document décrit les principes essentiels 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.

5.3 Normes spécifiant des exigences

5.3.1 ISO/IEC 27001

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Domaine d'application: Ce document spécifie les exigences relatives à l'établissement, à la mise en œuvre, à l'exploitation, à la surveillance, à la revue, à la maintenance et à l'amélioration des systèmes de management de la sécurité de l'information (SMSI) formalisés, dans le contexte des risques globaux liés à l'activité de l'organisme. Il spécifie les exigences relatives à la mise en œuvre de mesures de sécurité

de l'information adaptés aux besoins de chaque organisme ou de ses parties constitutives. Ce document peut être utilisé par tous les organismes, quels que soient leur type, leur taille et leur nature.

Objectif: L'ISO/IEC 27001 fournit des exigences normatives relatives à l'élaboration et à l'exploitation d'un SMSI, y compris un ensemble de mesures de sécurité destinées à la maîtrise et à l'atténuation des risques associés aux actifs informationnels que l'organisme cherche à protéger en mettant en œuvre son SMSI. Les organismes qui exploitent un SMSI peuvent faire auditer et certifier sa conformité. Les objectifs et mesures de sécurité définis dans l'ISO/IEC 27001:2013, Annexe A doivent être sélectionnés, en fonction des besoins, dans le cadre de ce processus de SMSI, pour satisfaire aux exigences identifiées. Les objectifs et mesures de sécurité répertoriés dans l'ISO/IEC 27001:2013, Tableau A.1 découlent directement de ceux qui sont répertoriés dans l'ISO/IEC 27002:2013, Articles 5 à 18, avec lesquels ils sont en adéquation.

5.3.2 ISO/IEC 27006

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Domaine d'application: Ce document spécifie des exigences et fournit des recommandations pour les organismes procédant à l'audit et à la certification de SMSI conformément à l'ISO/IEC 27001, en plus des exigences figurant dans l'ISO/IEC 17021. Il a pour principal objet de faciliter l'accréditation des organismes de certification qui procèdent à la certification de SMSI selon l'ISO/IEC 27001.

Le respect des exigences stipulées dans ce document doit être démontré en termes de compétences et de fiabilité par toute personne ou organisme habilité à procéder à la certification de SMSI, et les recommandations contenues dans ce document fournissent une interprétation supplémentaire de ces exigences pour toute personne ou organisme procédant à la certification de SMSI.

Objectif: L'ISO/IEC 27006 complète l'ISO/IEC 17021 en définissant les exigences permettant aux organismes de certification d'obtenir une accréditation et en les autorisant ainsi à délivrer des certifications de conformité satisfaisant aux exigences stipulées dans l'ISO/IEC 27001.

5.3.3 ISO/IEC 27009

Technologies de l'information — Techniques de sécurité — Application de l'ISO/IEC 27001 à un secteur spécifique — Exigences

Domaine d'application: Ce document définit les exigences relatives à l'utilisation de l'ISO/IEC 27001 dans n'importe quel secteur spécifique (domaine, domaine d'application ou secteur de marché). Il explique comment ajouter des exigences supplémentaires à celles définies dans l'ISO/IEC 27001, comment affiner les exigences de l'ISO/IEC 27001, et comment ajouter des mesures de sécurité ou des ensembles de mesures de sécurité à l'Annexe A de l'ISO/IEC 27001:2013.

Objectif: L'ISO/IEC 27009 permet de s'assurer que les exigences supplémentaires ou affinées ne sont pas en conflit avec les exigences de l'ISO/IEC 27001.

5.4 Normes décrivant des lignes directrices générales

5.4.1 ISO/IEC 27002

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information

Domaine d'application: Ce document fournit une liste d'objectifs de mesures de sécurité communément acceptées et des mesures de sécurité issues des bonnes pratiques à utiliser comme recommandations lors de la sélection et de la mise en œuvre des mesures de sécurité destinées à assurer la sécurité de l'information.

Objectif: L'ISO/IEC 27002 fournit des recommandations pour la mise en œuvre des mesures de sécurité de l'information. Les Articles 5 à 18, en particulier, fournissent des recommandations de mise en œuvre et des recommandations relatives aux bonnes pratiques qui accompagnent les mesures de sécurité spécifiées dans l'ISO/IEC 27001:2013, A.5 à A.18.

5.4.2 ISO/IEC 27003

Technologies de l'information — Techniques de sécurité — Système de management de la sécurité de l'information — Lignes directrices

Domaine d'application: Ce document fournit des explications et des recommandations concernant l'ISO/IEC 27001:2013.

Objectif: L'ISO/IEC 27003 fournit les bases pour la mise en œuvre réussie d'un SMSI conformément à l'ISO/IEC 27001.

5.4.3 ISO/IEC 27004

Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation

Domaine d'application: Ce document fournit des lignes directrices visant à aider les organismes à évaluer les performances en matière de sécurité de l'information et l'efficacité du SMSI afin de satisfaire aux exigences de l'ISO/IEC 27001:2013, 9.1. Il traite des points suivants:

a) la surveillance et le mesurage des performances en matière de sécurité de l'information;

b) la surveillance et le mesurage de l'efficacité d'un système de management de la sécurité de l'information (SMSI), y compris de ses processus et de ses mesures de sécurité;

c) l'analyse et l'évaluation des résultats de la surveillance et du mesurage.

Objectif: L'ISO/IEC 27004 fournit un cadre qui permet d'apprécier l'efficacité du SMSI qui doit être mesuré et évalué selon l'ISO/IEC 27001.

5.4.4 ISO/IEC 27005

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

Domaine d'application: Ce document fournit des lignes directrices pour la gestion des risques liés à la sécurité de l'information. L'approche décrite dans ce document vient étayer les concepts généraux énoncés dans l'ISO/IEC 27001.

Objectif: L'ISO/IEC 27005 fournit des recommandations pour la mise en œuvre d'une approche de gestion des risques orientée processus afin d'aider à la bonne mise en œuvre et à la satisfaction des exigences de gestion des risques liés à la sécurité de l'information de l'ISO/IEC 27001.

5.4.5 ISO/IEC 27007

Technologies de l'information — Techniques de sécurité — Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Domaine d'application: Ce document fournit des recommandations sur la réalisation des audits de SMSI, ainsi que sur les compétences des auditeurs de systèmes de management de la sécurité de l'information, en complément des recommandations figurant dans l'ISO 19011, qui sont applicables aux systèmes de management en général.

Objectif: L'ISO/IEC 27007 fournit des recommandations aux organismes qui doivent effectuer des audits internes ou externes sur un SMSI ou gérer un programme d'audit de SMSI conformément aux exigences spécifiées dans l'ISO/IEC 27001.

5.4.6 ISO/IEC TR 27008

Technologies de l'information — Techniques de sécurité — Lignes directrices pour les auditeurs des contrôles de sécurité de l'information

Domaine d'application: Ce document fournit des recommandations pour la revue de la mise en œuvre et de l'exploitation des mesures de sécurité, y compris le contrôle de la conformité technique des mesures de sécurité en place dans les systèmes d'information, conformément aux normes de sécurité de l'information établies d'un organisme.

Objectif: Ce document met l'accent sur les revues des mesures de sécurité de l'information, y compris le contrôle de leur conformité technique, par rapport à une norme relative à la mise en œuvre de la sécurité de l'information, établie par l'organisme. Il n'a pas pour objet de fournir des recommandations spécifiques sur le contrôle de la conformité en ce qui concerne le mesurage, l'appréciation du risque ou l'audit d'un SMSI tels que spécifiés dans l'ISO/IEC 27004, l'ISO/IEC 27005 ou l'ISO/IEC 27007, respectivement. Ce document n'est pas destiné à l'audit des systèmes de management.

5.4.7 ISO/IEC 27013

Technologies de l'information — Techniques de sécurité — Guide sur la mise en œuvre intégrée de l'ISO/IEC 27001 et l'*ISO/IEC 20000-1*

Domaine d'application: Ce document fournit des recommandations relatives à la mise en œuvre intégrée de l'ISO/IEC 27001 et de l'ISO/IEC 20000-1 aux organismes qui souhaitent:

a) mettre en œuvre l'ISO/IEC 27001 alors qu'ils ont déjà adopté l'ISO/IEC 20000-1, et vice-versa;

b) mettre en œuvre l'ISO/IEC 27001 et l'ISO/IEC 20000-1 simultanément;

c) intégrer les systèmes de management existants en fonction de l'ISO/IEC 27001 et de l'ISO/IEC 20000-1.

Ce document se concentre exclusivement sur la mise en œuvre intégrée d'un système de management de la sécurité de l'information (SMSI) tel que spécifié dans l'ISO/IEC 27001 et d'un système de management des services (SMS) tel que spécifié dans l'ISO/IEC 20000-1.

Dans la pratique, l'ISO/IEC 27001 et l'ISO/IEC 20000-1 peuvent également être intégrés à d'autres normes de système de management, telles que l'ISO 9001 et l'ISO 14001.

Objectif: Permettre aux organismes de mieux comprendre les caractéristiques, les ressemblances et les différences de l'ISO/IEC 27001 et de l'ISO/IEC 20000-1 afin de faciliter la planification d'un système de management intégré conforme à ces deux Normes internationales.

5.4.8 ISO/IEC 27014

Technologies de l'information — Techniques de sécurité — Gouvernance de la sécurité de l'information

Domaine d'application: Ce document fournit des recommandations sur des principes et des processus de gouvernance de la sécurité de l'information grâce auxquels les organismes peuvent évaluer, diriger et surveiller le management de la sécurité de l'information.

Objectif: La sécurité de l'information représente aujourd'hui un enjeu majeur pour les organismes. Ceux-ci ne sont pas seulement confrontés à des exigences réglementaires toujours plus nombreuses, ils savent également que l'échec des mesures de sécurité de l'information qu'ils mettent en place peut avoir un impact direct sur leur réputation. C'est pourquoi les instances dirigeantes, dans le cadre de leurs

responsabilités en matière de gouvernance, doivent de plus en plus souvent superviser la sécurité de l'information afin d'assurer l'atteinte des objectifs de l'organisme.

5.4.9 ISO/IEC TR 27016

Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Économie organisationnelle

Domaine d'application: Ce document fournit une méthodologie qui permet aux organismes de mieux comprendre, d'un point de vue économique, comment évaluer avec plus de précision les actifs informationnels identifiés, évaluer les risques pesant potentiellement sur ces actifs informationnels, apprécier la valeur apportée par les mesures de sécurité de la protection de l'information à ces actifs informationnels et déterminer le niveau optimal de ressources à mettre en œuvre pour assurer la sécurité de ces actifs informationnels.

Objectif: Ce document vient compléter la famille de normes du SMSI en ajoutant un point de vue économique à la protection des actifs informationnels d'un organisme dans le contexte plus général de l'environnement sociétal dans lequel il évolue, et en fournissant des recommandations concernant la manière d'appliquer l'économie organisationnelle de la sécurité de l'information par le biais de modèles et d'exemples.

5.4.10 ISO/IEC 27021

Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Exigences de compétence pour les professionnels de la gestion des systèmes de management de la sécurité de l'information

Domaine d'application: Ce document spécifie les exigences de compétence pour les professionnels SMSI impliqués, en tant que responsables ou collaborateurs, dans l'établissement, la mise en œuvre, la maintenance et l'amélioration continue d'un ou plusieurs processus de système de management de la sécurité de l'information conformes à l'ISO/IEC 27001:2013.

Objectif: Ce document est destiné:

a) aux individus qui souhaitent démontrer leurs compétences en tant que professionnels SMSI (système de management de la sécurité de l'information), ou qui souhaitent comprendre et acquérir les compétences requises pour travailler dans ce domaine, et souhaitent élargir leurs connaissances;

b) aux organismes qui sont à la recherche de candidats professionnels SMSI potentiels en vue de définir les compétences requises pour pourvoir des postes assumant des rôles liés au SMSI;

c) aux organismes chargés de développer une certification pour les professionnels SMSI qui ont besoin de disposer d'un ensemble de connaissances pour les sources d'examen; et

d) aux organismes d'éducation et de formation, tels que les universités et les établissements d'enseignement professionnel, afin qu'ils adaptent leurs programmes d'études et leurs cours aux compétences requises pour les professionnels SMSI.

5.5 Normes décrivant des lignes directrices propres à un secteur

5.5.1 ISO/IEC 27010

Technologies de l'information — Techniques de sécurité — Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles

Domaine d'application: Ce document fournit des lignes directrices qui complètent les recommandations contenues dans la famille de normes ISO/IEC 27000 relatives à la mise en œuvre du management de la sécurité de l'information au sein des communautés de partage d'informations.

Ce document, en outre, des mesures de sécurité et des recommandations portant plus précisément sur la mise en place, la mise en œuvre, le maintien et l'amélioration de la sécurité de l'information dans les communications interorganisationnelles et intersectorielles.

Objectif: Ce document est applicable à toutes les formes d'échange et de partage d'informations sensibles, privées et publiques, sur le plan national et international, au sein d'une même branche d'activité/d'un même secteur de marché ou entre un secteur et un autre. Il peut en particulier s'appliquer aux échanges et aux partages d'informations se rapportant à la fourniture, à la maintenance et à la protection de l'infrastructure critique d'un organisme ou d'un État.

5.5.2 ISO/IEC 27011

Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour les contrôles de la sécurité de l'information fondés sur l'ISO/IEC 27002 pour les organismes de télécommunications

Domaine d'application: Ce document fournit des lignes directrices relatives à la mise en œuvre des mesures de sécurité de l'information dans les organismes de télécommunications.

Objectif: L'ISO/IEC 27011 permet aux organismes de télécommunications de satisfaire aux exigences de référence de management de la sécurité de l'information concernant la confidentialité, l'intégrité, la disponibilité et toute autre propriété de sécurité pertinente.

5.5.3 ISO/IEC 27017

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Domaine d'application: L'ISO/IEC 27017 contient des lignes directrices relatives aux mesures de sécurité de l'information applicables à la prestation et à l'utilisation de services d'informatique en nuage, par exemple:

— des recommandations supplémentaires concernant la mise en œuvre des mesures de sécurité pertinentes spécifiées dans l'ISO/IEC 27002;

— des mesures de sécurité supplémentaires et des recommandations de mise en œuvre spécifiquement liés aux services d'informatique en nuage.

Objectif: Ce document fournit des recommandations concernant les mesures de sécurité et la mise en œuvre destinées aux prestataires de services d'informatique en nuage et à leurs clients.

5.5.4 ISO/IEC 27018

Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Domaine d'application: L'ISO/IEC 27018 établit des objectifs de mesure de sécurité communément acceptés, des mesures de sécurité et des lignes directrices de mise en œuvre de mesures destinées à protéger les informations personnelles identifiables (PII) conformément aux principes de respect de la vie privée de l'ISO/IEC 29100 pour l'environnement informatique en nuage public.

Objectif: Ce document s'applique aux organismes, y compris les sociétés publiques et privées, les entités gouvernementales et les organismes à but non lucratif, qui offrent des services de traitement de l'information en tant que processeurs de PII via l'informatique en nuage sous contrat auprès d'autres organismes. Les lignes directrices de ce document peuvent également s'appliquer aux organismes agissant en tant que contrôleurs de PII. Toutefois, les contrôleurs de PII peuvent être soumis à une législation, des règlements et des obligations supplémentaires en matière de protection des PII qui ne s'appliquent pas aux processeurs de PII, et ceux-ci ne sont pas couverts dans ce document.

5.5.5 ISO/IEC 27019

Technologie de l'information — Techniques de sécurité — Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie

Domaine d'application: Ce document contient des recommandations basées sur l'ISO/IEC 27002:2013 applicables aux systèmes de contrôle des processus utilisés par les opérateurs énergétiques pour contrôler et surveiller la production ou la génération, la transmission, le stockage et la distribution de l'énergie électrique, du gaz et de la chaleur, ainsi que dans le cadre du contrôle des processus associés. Cela inclut en particulier les équipements suivants:

— technologie informatique générale de contrôle, de surveillance et d'automatisation des processus, centrale et distribuée, et systèmes informatiques utilisés pour son exploitation, tels que les dispositifs de programmation et de paramétrage;

— contrôleurs numériques et composants d'automatisation tels que les dispositifs de contrôle et de terrain ou les automates programmables, y compris les éléments de capteurs et organes de commande numériques;

— tous les autres systèmes informatiques utilisés pour prendre en charge le domaine du contrôle des processus, par exemple pour les tâches de visualisation de données supplémentaires et à des fins de contrôle, de surveillance, d'archivage de données, de consignation d'historiques, de génération de rapports et de documentation;

— technologie de communications utilisée dans le domaine du contrôle des processus, par exemple les réseaux, la télémesure, les applications de téléconduite et les technologies de commande à distance;

— composants d'infrastructures de compteurs avancées (ICA), tels que les compteurs intelligents;

— dispositifs de mesurage, destinés par exemple à mesurer les valeurs d'émission;

— systèmes numériques de protection et de sécurité, tels que les relais de protection ou les API de sécurité, régulateurs d'urgence;

— systèmes de management de l'énergie, par exemple, de ressources énergétiques distribuées (DER), infrastructures de recharge électrique, chez les particuliers, dans les bâtiments d'habitation ou dans les installations de clients industriels;

— composants distribués d'environnements de réseaux intelligents, par exemple dans les réseaux électriques, chez les particuliers, dans les bâtiments d'habitation ou dans les installations de clients industriels;

— tous les logiciels, micrologiciels et applications installés sur les systèmes mentionnés ci-dessus, par exemple, applications DMS (système de gestion de la distribution) ou OMS (système de gestion des pannes);

— tous les locaux hébergeant les équipements et les systèmes mentionnés ci-dessus;

— systèmes de maintenance à distance pour les systèmes mentionnés ci-dessus.

Ce document ne s'applique pas au domaine du contrôle de processus des installations nucléaires. Ce domaine est couvert par l'IEC 62645.

Ce document contient également une exigence relative à l'adaptation de l'appréciation du risque et des processus de traitement décrits dans l'ISO/IEC 27001:2013 aux recommandations spécifiques à l'industrie des opérateurs énergétiques fournies dans le présent document.

Objectif: Outre les objectifs et mesures de sécurité présentés dans l'ISO/IEC 27002, ce document contient des lignes directrices concernant les systèmes utilisés par les opérateurs énergétiques et les fournisseurs d'énergie et relatives aux mesures de sécurité de l'information répondant à d'autres exigences spéciales.

5.5.6 ISO 27799

Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002

Domaine d'application: Ce document fournit des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, notamment en ce qui concerne la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte l'environnement à risques pour la sécurité de l'information de l'organisme.

Ce document fournit des recommandations pour la mise en œuvre des mesures de sécurité décrites dans l'ISO/IEC 27002 et les complète lorsque cela s'avère nécessaire, de sorte qu'ils puissent être effectivement utilisés pour le management de la sécurité des informations de santé.

Objectif: L'ISO 27799 propose aux organismes de santé une adaptation des lignes directrices de l'ISO/IEC 27002 propres à leur cœur de métier, qui s'ajoutent aux recommandations fournies pour satisfaire aux exigences de l'ISO/IEC 27001:2013, Annexe A.

Bibliographie

[1] ISO 9000:2015, *Systèmes de management de la qualité — Principes essentiels et vocabulaire*

[2] ISO/IEC IEEE 15939:2017, *Ingénierie des systèmes et du logiciel — Processus de mesure*

[3] ISO/IEC 17021, *Évaluation de la conformité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management*

[4] ISO 19011:2011, *Lignes directrices pour l'audit des systèmes de management*

[5] ISO/IEC 20000-1:2011, *Technologies de l'information — Gestion des services — Partie 1: Exigences du système de management des services*

[6] ISO/IEC 27001, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences*

[7] ISO/IEC 27002, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information*

[8] ISO/IEC 27003, *Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Lignes directrices*

[9] ISO/IEC 27004, *Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Surveillance, mesurage, analyse et évaluation*

[10] ISO/IEC 27005, *Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information*

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

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

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

[14] ISO/IEC 27009, *Technologies de l'information — Techniques de sécurité — Application de l'ISO/IEC 27001 à un secteur spécifique — Exigences*

[15] ISO/IEC 27010, *Technologies de l'information — Techniques de sécurité — Gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles*

[16] ISO/IEC 27011, *Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour les contrôles de la sécurité de l'information fondés sur l'ISO/IEC 27002 pour les organismes de télécommunications*

[17] ISO/IEC 27013, *Technologies de l'information — Techniques de sécurité — Guide sur la mise en œuvre intégrée d'ISO/IEC 27001 et ISO/IEC 20000-1*

[18] ISO/IEC 27014, *Technologies de l'information — Techniques de sécurité — Gouvernance de la sécurité de l'information*

[19] ISO/IEC/TR 27016, *Technologies de l'information — Techniques de sécurité — Management de la sécurité de l'information — Économie organisationnelle*

[20] ISO/IEC 27017, *Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage*

[21] ISO/IEC 27018, *Technologies de l'information — Techniques de sécurité — Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII*

[22] ISO/IEC 27019, *Technologies de l'information — Techniques de sécurité — Mesures de sécurité de l'information pour l'industrie des opérateurs de l'énergie*

[23] ISO/IEC 27021, *Technologies de l'information — Techniques de sécurité — Exigences de compétence pour les professionnels de la gestion des systèmes de management de la sécurité*

[24] ISO 27799, *Informatique de santé — Management de la sécurité de l'information relative à la santé en utilisant l'ISO/IEC 27002*

[25] Guide ISO 73:2009, *Management du risque — Vocabulaire*

ICS 01.040.35; 03.100.70; 35.030

Prix basé sur 27 pages