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

ISO/IEC 27000:2018 - Preview only Copy via ILNAS e-Shop

Numéro de référence
ISO/IEC 27000:2018(F)

© ISO/IEC 2018

ISO/IEC 27000:2018 - Preview only Copy via ILNAS e-Shop

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 27000:2018 - Preview only Copy via ILNAS e-Shop

© 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 27000:2018 - Preview only Copy via ILNAS e-Shop

 © 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 27000:2018 - Preview only Copy via ILNAS e-Shop

© ISO/IEC 2018 – Tous droits réservés

ISO/IEC 27000:2018 - Preview only Copy via ILNAS e-Shop

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/IEC 27000:2018 - Preview only Copy via ILNAS e-Shop

© ISO 2018 – Tous droits réservés