
**Technologies de l'information —
Techniques de sécurité — Systèmes de
gestion de sécurité de l'information —
Vue d'ensemble et vocabulaire**

*Information technology — Security techniques — Information
security management systems — Overview and vocabulary*



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2016, Publié en Suisse

Droits de reproduction réservés. Sauf indication contraire, 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, l'affichage sur l'internet ou sur un Intranet, sans autorisation écrite préalable. Les demandes d'autorisation peuvent être adressées à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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

Sommaire

Page

Avant-propos	v
0 Introduction	1
0.1 Vue d'ensemble.....	1
0.2 La famille de normes du SMSI.....	1
0.3 Objet de la présente Norme internationale.....	2
1 Domaine d'application	2
2 Termes et définitions	3
3 Systèmes de management de la sécurité de l'information	15
3.1 Généralités.....	15
3.2 Qu'est-ce qu'un SMSI?.....	15
3.2.1 Vue d'ensemble et principes.....	15
3.2.2 L'information.....	16
3.2.3 Sécurité de l'information.....	16
3.2.4 Management.....	17
3.2.5 Système de management.....	17
3.3 Approche processus.....	17
3.4 Raisons expliquant pourquoi un SMSI est important.....	17
3.5 Établissement, surveillance, maintenance et amélioration d'un SMSI.....	18
3.5.1 Vue d'ensemble.....	18
3.5.2 Identifier les exigences liées à la sécurité de l'information.....	19
3.5.3 Apprécier les risques liés à la sécurité de l'information.....	19
3.5.4 Traiter les risques liés à la sécurité de l'information.....	20
3.5.5 Sélectionner et mettre en œuvre les mesures de sécurité.....	20
3.5.6 Surveiller, mettre à jour et améliorer l'efficacité du SMSI.....	21
3.5.7 Amélioration continue.....	21
3.6 Facteurs critiques de succès du SMSI.....	22
3.7 Avantages de la famille de normes du SMSI.....	22
4 La famille de normes du SMSI	23
4.1 Information générales.....	23
4.2 Normes donnant une vue d'ensemble et décrivant la terminologie.....	24
4.2.1 ISO/IEC 27000 (la présente Norme internationale).....	24
4.3 Normes spécifiant des exigences.....	24
4.3.1 ISO/IEC 27001.....	24
4.3.2 ISO/IEC 27006.....	24
4.4 Normes décrivant des lignes directrices générales.....	25
4.4.1 ISO/IEC 27002.....	25
4.4.2 ISO/IEC 27003.....	25
4.4.3 ISO/IEC 27004.....	25
4.4.4 ISO/IEC 27005.....	25
4.4.5 ISO/IEC 27007.....	25
4.4.6 ISO/IEC/TR 27008.....	26
4.4.7 ISO/IEC 27013.....	26
4.4.8 ISO/IEC 27014.....	26
4.4.9 ISO/IEC/TR 27016.....	27
4.5 Normes décrivant des lignes directrices propres à un secteur.....	27
4.5.1 ISO/IEC 27010.....	27
4.5.2 ISO/IEC 27011.....	27
4.5.3 ISO/IEC/TR 27015.....	27
4.5.4 ISO/IEC 27017.....	28
4.5.5 ISO/IEC 27018.....	28
4.5.6 ISO/IEC/TR 27019.....	28
4.5.7 ISO 27799.....	29

Annexe A (informative) Formes verbales utilisées pour exprimer des dispositions	30
Annexe B (informative) Termes et propriété des termes	31
Bibliographie	35

Avant-propos

L'ISO (Organisation internationale de normalisation) et l'IEC (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de l'IEC participent à l'élaboration de Normes internationales par l'intermédiaire de comités techniques créés par l'organisme concerné pour traiter de domaines particuliers à une activité technique. Les comités techniques de l'ISO et de l'IEC collaborent dans des domaines d'intérêt commun. D'autres organismes internationaux, gouvernementaux et non gouvernementaux, en liaison avec l'ISO et l'IEC participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

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 document. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir <http://www.iso.org/directives>).

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO 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 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'OMC concernant les obstacles techniques au commerce (OTC), voir le lien suivant: [Avant-propos — Informations supplémentaires](#).

Le comité chargé de l'élaboration du présent document est l'ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette quatrième édition annule et remplace la troisième édition (ISO/IEC 27000:2014), qui a fait l'objet d'une révision technique.