NORME INTERNATIONALE

ISO/CEI 27000

Troisième édition
2014-01-15

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

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

Numéro de référence
ISO/CEI 27000:2014(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Publié en Suisse

Sommaire

Page

Avant-propos ..... **iv**

0 Introduction ..... **v**

1 Domaine d'application **1**

2 Termes et définitions **1**

3 Systèmes de management de la sécurité de l'information **13**
3.1 Introduction 13
3.2 Qu'est-ce qu'un SMSI ? 13
3.3 Approche processus 15
3.4 Raisons pour lesquelles un SMSI est important 15
3.5 Établissement, surveillance, mise à jour et amélioration d'un SMSI 16
3.6 Facteurs critiques de succès du SMSI 19
3.7 Avantages de la famille de normes du SMSI 20

4 La famille de normes du SMSI **20**
4.1 Informations générales 20
4.2 Normes décrivant une vue d'ensemble et une terminologie 21
4.3 Normes spécifiant des exigences 22
4.4 Normes décrivant des lignes directrices générales 22
4.5 Normes décrivant des lignes directrices propres à un secteur 25

Annexe A (informative) **Formes verbales pour exprimer des dispositions** **27**

Annexe B (informative) **Termes et propriété des termes** **28**

Bibliographie **32**

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 de leur compétence. 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 Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale du comité technique mixte est d'élaborer des Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication en tant que Normes internationales requiert l'approbation d'au moins 75 % des organismes nationaux votants.

L'attention est appelée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/IEC 27000 a été élaborée par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27000:2012), qui a fait l'objet d'une révision technique.

0 Introduction

0.1 Vue d'ensemble

Les Normes internationales relatives aux systèmes de management fournissent un modèle en matière d'établissement et d'exploitation d'un système de management. Ce modèle comprend les caractéristiques que les experts dans le domaine s'accordent à reconnaître comme reflétant l'état de l'art au niveau international. Le sous-comité ISO/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. Elles peuvent également utiliser ces normes pour se préparer à une évaluation indépendante de leurs SMSI en matière de protection de l'information.

0.2 La famille de normes du SMSI

La famille de normes du SMSI (voir l'Article 4) a pour objet d'aider les organismes de tous types et de toutes tailles à déployer et à exploiter un SMSI. Elle se compose des Normes internationales suivantes (indiquées ci-dessous par ordre numérique) regroupées sous le titre général *Technologies de l'information — Techniques de sécurité*:

— ISO/IEC 27000, *Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

— ISO/IEC 27001, *Systèmes de management de la sécurité de l'information — Exigences*

— ISO/IEC 27002, *Code de bonne pratique pour les mesures de sécurité de l'information*

— ISO/IEC 27003, *Lignes directrices pour la mise en oeuvre du système de management de la sécurité de l'information*

— ISO/IEC 27004, *Management de la sécurité de l'information — Mesurage*

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

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

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

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

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

— ISO/IEC 27011, *Lignes directrices du management de la sécurité de l'information pour les organismes de télécommunications sur la base de l'*ISO/IEC 27002

— ISO/IEC 27013, *Guide sur la mise en oeuvre intégrée de* l'ISO/IEC 27001 *et de l'*ISO/IEC 20000-1

— ISO/IEC 27014, *Gouvernance de la sécurité de l'information*

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

— ISO/IEC/TR 27016, *Management de la sécurité de l'information — Économie organisationnelle*

NOTE Le titre général «*Technologies de l'information — Techniques de sécurité*» indique que ces normes ont été élaborées par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Les Normes internationales qui font également partie de la famille de normes du SMSI, mais qui ne sont pas regroupées sous le même titre général, sont les suivantes:

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

0.3 Objet de la présente Norme internationale

La présente Norme internationale offre une vue d'ensemble des systèmes de management de la sécurité de l'information et définit les termes qui s'y rapportent.

NOTE L'Annexe A fournit des éclaircissements sur la façon dont les formes verbales sont utilisées pour exprimer des exigences et/ou des préconisations dans la famille de normes du SMSI.

La famille de normes du SMSI comporte des normes qui:

a) définissent les exigences pour un SMSI et pour les organismes certifiant de tels systèmes;

b) apportent un soutien direct, des préconisations détaillées et/ou une interprétation du processus général visant à établir, mettre en œuvre, entretenir et améliorer un SMSI;

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

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

Les termes et les définitions fournis dans la présente Norme internationale:

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

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

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

