Norme belge

ISO/IEC 27000:2016

NBN ISO/IEC 27000:2016

Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Vue d'ensemble et vocabulaire (ISO/IEC 27000:2016)

Valable à partir de 22-04-2016

Remplace NBN ISO/IEC 27000:2014

ICS: 01.040.35, 35.040

Bureau de Normalisation
Rue Joseph-II 40 bte 6
1000 Bruxelles

T. +32 2 738 01 11
F. +32 2 733 42 64
info@nbn.be

BTW BE0880.857.592
IBAN BE69 6790 0009 5178
BIC Code PCHQBEBB

www.nbn.be

NORME INTERNATIONALE

ISO/IEC 27000

Quatrième édition
2016-02-15

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

Numéro de référence
ISO/IEC 27000:2016(F)

ISO/IEC 27000:2016(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

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

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.

NORME INTERNATIONALE **ISO/IEC 27000:2016(F)**

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

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. Ils 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 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 bonnes pratiques pour le management de la sécurité de l'information*

— ISO/IEC 27003, *Lignes directrices pour la mise en œuvre 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 27009, *Application de l'*ISO/IEC 27001 *à un secteur spécifique — Exigences*

— 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 œuvre intégrée de l'*ISO/IEC 27001 *et* 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*

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

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

— ISO/IEC 27019, *Lignes directrices de management de la sécurité de l'information fondées sur l'*ISO/IEC 27002 *pour les systèmes de contrôle des processus spécifiques à l'industrie de l'énergie*

NOTE Le titre général « *Technologies de l'information — Techniques de sécurité* » indique que ces Normes internationales 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, *Informatique de santé — Management 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 relatives à un SMSI et à ceux qui certifient de tels systèmes;

b) apportent des informations directes, des préconisations 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.

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.

1 Domaine d'application

La présente Norme internationale offre une vue d'ensemble des systèmes de management de la sécurité de l'information, ainsi que des termes et définitions d'usage courant dans la famille de normes du SMSI.

La présente Norme internationale 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).

2 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent:

2.1
contrôle d'accès
moyens mis en œuvre pour assurer que l'accès aux actifs est autorisé et limité selon les *exigences* (2.63) propres à la sécurité et à l'activité métier

2.2
modèle analytique
algorithme ou calcul combinant une ou plusieurs *mesures élémentaires* (2.10) et/ou *mesures dérivées (2.22)* avec les *critères de décision* associés (2.21)

2.3
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

2.4
attribut
propriété ou caractéristique d'un *objet* (2.55) qui peut être distingué quantitativement ou qualitativement par des moyens humains ou automatiques

[SOURCE: ISO/IEC 15939:2007, 2.2, modifiée — Le terme « entité » a été remplacé par « objet » dans la définition.]

2.5
audit
processus (2.61) méthodique, indépendant et documenté 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: Les termes « preuves d'audit » et « critères d'audit » sont définis dans l'ISO 19011.

2.6
champ de l'audit
étendue et limites d'un *audit* (2.5)

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

2.7
authentification
méthode permettant de garantir qu'une caractéristique revendiquée pour une entité est correcte

2.8
authenticité
propriété selon laquelle une entité est ce qu'elle revendique être

2.9
disponibilité
propriété d'être accessible et utilisable à la demande par une entité autorisée