ICS: 35.040

norme belge enregistrée

NBN ISO/IEC 27001

1e éd., juin 2014

Indice de classement: Z 07

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2013)

Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen (ISO/IEC 27001:2013)

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013)

Autorisation de publication: 20 juin 2014

La présente norme ISO/IEC 27001:2013 a le statut d'une norme belge.

La présente norme existe en deux versions officielles (anglais, français).

standards for .be

Bureau de Normalisation - rue Joseph II 40 - 1000 Bruxelles - Belgique
Tél: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be
Banque 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB TVA BE0880857592

Prix: groupe 28

ICS: 35.040

Geregistreerde Belgische norm

NBN ISO/IEC 27001

1e uitg., juni 2014

Normklasse: Z 07

Informatietechnologie - Beveiligingstechnieken - Managementsystemen voor informatiebeveiliging - Eisen (ISO/IEC 27001:2013)

Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences (ISO/IEC 27001:2013)

Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2013)

Toelating tot publicatie: 20 juni 2014

Deze norm ISO/IEC 27001:2013 heeft de status van een Belgische norm.

Deze norm bestaat in twee officiële versies (Engels, Frans).

standards for .be

Bureau voor Normalisatie - Jozef II-straat 40 - 1000 Brussel - België
Tel: +32 2 738 01 11 - Fax: +32 2 733 42 64 - E-mail: info@nbn.be - NBN Online: www.nbn.be
Bank 679-0000951-78 IBAN BE69 6790 0009 5178 BIC PCHQBEBB BTW BE0880857592

Prijsgroep: 28

NBN ISO/IEC 27001 (2014)

NORME INTERNATIONALE

ISO/CEI 27001

Deuxième édition
2013-10-01

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

Information technology — Security techniques — Information security management systems — Requirements

Numéro de référence
ISO/CEI 27001:2013(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

Version française parue en 2013

Publié en Suisse

Sommaire

Page

Avant-propos

L'ISO (Organisation internationale de normalisation) et la CEI (Commission électrotechnique internationale) forment le système spécialisé de la normalisation mondiale. Les organismes nationaux membres de l'ISO ou de la CEI participent au développement de Normes internationales par l'intermédiaire des comités techniques créés par l'organisation concernée afin de s'occuper des domaines particuliers de l'activité technique. Les comités techniques de l'ISO et de la CEI collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO et la CEI participent également aux travaux. Dans le domaine des technologies de l'information, l'ISO et la CEI ont créé un comité technique mixte, l'ISO/CEI JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/CEI, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins 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 la CEI ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27001 a été élaborée par le comité technique mixte ISO/CEI JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Cette deuxième édition annule et remplace la première édition (ISO/CEI 27001:2005), qui a fait l'objet d'une révision technique.

0 Introduction

0.1 Généralités

La présente Norme internationale a été élaborée pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l'information. L'adoption d'un système de management de la sécurité de l'information relève d'une décision stratégique de l'organisation. L'établissement et la mise en œuvre d'un système de management de la sécurité de l'information d'une organisation tiennent compte des besoins et des objectifs de l'organisation, des exigences de sécurité, des processus organisationnels mis en œuvre, ainsi que de la taille et de la structure de l'organisation. Tous ces facteurs d'influence sont appelés à évoluer dans le temps.

Le système de management de la sécurité de l'information préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate.

Il est important que le système de management de la sécurité de l'information fasse partie intégrante des processus et de la structure de management d'ensemble de l'organisation et que la sécurité de l'information soit prise en compte dans la conception des processus, des systèmes d'information et des mesures. Il est prévu qu'un système de management de la sécurité de l'information évolue conformément aux besoins de l'organisation.

La présente Norme internationale peut être utilisée par les parties internes et externes pour évaluer la capacité de l'organisation à répondre à ses propres exigences en matière de sécurité de l'information.

L'ordre dans lequel les exigences sont présentées dans la présente Norme internationale ne reflète pas leur importance, ni l'ordre dans lequel elles doivent être mises en œuvre. Les éléments des listes sont énumérés uniquement à des fins de référence.

L'ISO/CEI 27000 décrit une vue d'ensemble et le vocabulaire des systèmes de management de la sécurité de l'information, en se référant à la famille des normes du système de management de la sécurité de l'information (incluant l'ISO/CEI 27003,[2] l'ISO/CEI 27004[3] et l'ISO/CEI 27005[4]) avec les termes et les définitions qui s'y rapportent.

0.2 Compatibilité avec d'autres systèmes de management

La présente Norme internationale applique la structure de haut niveau, les titres de paragraphe identiques, le texte, les termes communs et les définitions fondamentales définies dans l'Annexe SL des Directives ISO/CEI, Partie 1, Supplément ISO consolidé, et, par conséquent, est compatible avec les autres normes de systèmes de management qui se conforment à l'Annexe SL.

Cette approche commune définie dans l'Annexe SL sera utile aux organisations qui choisissent de mettre en œuvre un système de management unique pour répondre aux exigences de deux ou plusieurs normes de systèmes de management.

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

1 Domaine d'application

La présente Norme internationale spécifie les exigences relatives à l'établissement, à la mise en œuvre, à la mise à jour et à l'amélioration continue d'un système de management de la sécurité de l'information dans le contexte d'une organisation. La présente Norme internationale comporte également des exigences sur l'appréciation et le traitement des risques de sécurité de l'information, adaptées aux besoins de l'organisation. Les exigences fixées dans la présente Norme internationale sont génériques et prévues pour s'appliquer à toute organisation, quels que soient son type, sa taille et sa nature. Il n'est pas admis qu'une organisation s'affranchisse de l'une des exigences spécifiées aux Articles 4 à 10 lorsqu'elle revendique la conformité à la présente Norme internationale.

2 Références normatives

Les documents suivants, en tout ou partie, sont référencés de manière normative dans le présent document et sont indispensables à son application. Pour les références datées, seule l'édition citée s'applique. Pour les références non datées, la dernière édition du document de référence s'applique (y compris les éventuels amendements).

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

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions fournis dans la norme ISO/CEI 27000 s'appliquent.

4 Contexte de l'organisation

4.1 Compréhension de l'organisation et de son contexte

L'organisation doit déterminer les enjeux externes et internes pertinents compte tenu de sa mission et qui influent sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son système de management de la sécurité de l'information.

NOTE Déterminer ces enjeux revient à établir le contexte externe et interne de l'organisation étudié dans le paragraphe 5.3 de l'ISO 31000:2009.[5]

4.2 Compréhension des besoins et des attentes des parties intéressées

L'organisation doit déterminer:

a) les parties intéressées qui sont concernées par le système de management de la sécurité de l'information; et

b) les exigences de ces parties intéressées concernant la sécurité de l'information.

NOTE Les exigences des parties intéressées peuvent inclure des exigences légales et réglementaires et des obligations contractuelles.