Norme belge

ISO/IEC 27005:2018

NBN ISO/IEC 27005:2018

Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information

Valable à partir de 27-11-2018

Remplace NBN ISO/IEC 27005:2014

ICS: 03.100.70, 35.030

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 BE41 0003 2556 2110
BIC Code BPOTBEB1

www.nbn.be

NORME INTERNATIONALE

ISO/IEC 27005

Troisième édition
2018-07

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

Information technology — Security techniques — Information security risk management

Numéro de référence
ISO/IEC 27005:2018(F)

DOCUMENT PROTÉGÉ PAR COPYRIGHT

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +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

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 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 l'IEC collaborent dans des domaines d'intérêt commun. D'autres organisations internationales, gouvernementales et non gouvernementales, 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 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 et l'IEC ne sauraient être tenues pour responsables 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 www.iso.org/avant-propos.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*.

Il convient que l'utilisateur adresse tout retour d'information ou toute question concernant le présent document à l'organisme national de normalisation de son pays. Une liste exhaustive desdits organismes se trouve à l'adresse www.iso.org/fr/members.html.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 27005:2011) qui a fait l'objet d'une révision technique.

Les principales modifications par rapport à l'édition précédente sont les suivantes:

— toutes les références directes à l'ISO/IEC 27001:2005 ont été supprimées;

— une information claire a été ajoutée, stipulant que le présent document ne contient pas de préconisations directes concernant la mise en œuvre des exigences du SMSI spécifiées dans l'ISO/IEC 27001 (voir Introduction);

— l'ISO/IEC 27001:2005 a été supprimée de l'Article 2;

— l'ISO/IEC 27001 a été ajoutée à la Bibliographie;

— l'Annexe G et toutes les références à cette Annexe ont été supprimées;

— des modifications éditoriales ont été effectuées en conséquence.

Introduction

Le présent document contient des lignes directrices relatives à la gestion des risques en sécurité de l'information dans un organisme. Cependant, le présent document ne fournit aucune méthodologie spécifique à la gestion des risques en sécurité de l'information. Il est du ressort de chaque organisme de définir son approche de la gestion des risques, en fonction, par exemple, du périmètre d'un système de management de la sécurité de l'information (SMSI), de ce qui existe dans l'organisme dans le domaine de la gestion des risques, ou encore de son secteur industriel. Plusieurs méthodologies existantes peuvent être utilisées en cohérence avec le cadre décrit dans le présent document pour appliquer les exigences du SMSI. Le présent document est fondé sur la méthode d'identification des risques liés à des actifs, des menaces et des vulnérabilités, qui n'est plus exigée par l'ISO/IEC 27001; il existe d'autres approches qui peuvent être utilisées.

Le présent document ne contient pas de préconisations directes concernant la mise en œuvre des exigences du SMSI spécifiées dans l'ISO/IEC 27001.

Le présent document s'adresse aux responsables et aux personnels concernés par la gestion des risques en sécurité de l'information au sein d'un organisme et, le cas échéant, aux tiers prenant part à ces activités.

NORME INTERNATIONALE **ISO/IEC 27005:2018(F)**

Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information

1 Domaine d'application

Le présent document contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.

Le présent document appuie les concepts généraux énoncés dans l'ISO/IEC 27001; il est conçu pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques.

Il est important de connaître les concepts, les modèles, les processus et les terminologies décrites dans l'ISO/IEC 27001 et l'ISO/IEC 27002 afin de bien comprendre le présent document.

Le présent document est applicable à tous types d'organismes (par exemple les entreprises commerciales, les agences gouvernementales, les organisations à but non lucratif) qui ont l'intention de gérer des risques susceptibles de compromettre la sécurité des informations de l'organisme.

2 Références normatives

Les documents suivants cités dans le texte constituent, pour tout ou partie de leur contenu, des exigences du présent document. 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/IEC 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 les définitions de l'ISO/IEC 27000 s'appliquent.

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/

4 Structure du présent document

Le présent document contient la description du processus de gestion des risques en sécurité de l'information et la description de ses activités.

Les informations générales sont fournies dans l'Article 5.

Un aperçu général du processus de gestion des risques en sécurité de l'information est donné dans l'Article 6.

Toutes les activités liées à la gestion des risques en sécurité de l'information, telles que présentées dans l'Article 6, sont ensuite décrites dans les articles suivants:

— établissement du contexte dans l'Article 7;