NORME INTERNATIONALE

ISO/CEI 27005

Deuxième édition
2011-06-01

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/CEI 27005:2011(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) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'élaboration des Normes internationales est en général confiée aux comités techniques de l'ISO. Chaque comité membre intéressé par une étude a le droit de faire partie du comité technique créé à cet effet. Les organisations internationales, gouvernementales et non gouvernementales, en liaison avec l'ISO participent également aux travaux. L'ISO collabore étroitement avec la Commission électrotechnique internationale (CEI) en ce qui concerne la normalisation électrotechnique.

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

La tâche principale des comités techniques est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par les comités techniques sont soumis aux comités membres pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des comités membres 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 ne saurait être tenue pour responsable de ne pas avoir identifié de tels droits de propriété et averti de leur existence.

L'ISO/CEI 27005 a été élaborée par le comité technique 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 27005:2008), qui a fait l'objet d'une révision technique.

Introduction

La présente Norme internationale contient des lignes directrices relatives à la gestion des risques en sécurité de l'information dans une organisation, qui viennent notamment en appui des exigences d'un SMSI (système de management de la sécurité de l'information) tel que défini dans l'ISO/CEI 27001. Cependant, la présente Norme internationale ne fournit aucune méthodologie spécifique à la gestion des risques en sécurité de l'information. Il est du ressort de chaque organisation de définir son approche de la gestion des risques, en fonction, par exemple, du périmètre du SMSI, de ce qui existe dans l'organisation 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 la présente Norme internationale pour appliquer les exigences du SMSI.

La présente Norme internationale s'adresse aux responsables et aux personnels concernés par la gestion des risques en sécurité de l'information au sein d'une organisation et, le cas échéant, aux tiers prenant part à ces activités.

Technologies de l'information — Techniques de sécurité — Gestion des risques en sécurité de l'information

1 Domaine d'application

La présente Norme internationale contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.

La présente Norme internationale vient en appui des concepts généraux énoncés dans l'ISO/CEI 27001; elle est conçue 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/CEI 27001 et l'ISO/CEI 27002 afin de bien comprendre la présente Norme internationale.

La présente Norme internationale est applicable à tous types d'organisations (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'organisation.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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/CEI 27000, *Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Vue d'ensemble et vocabulaire*

ISO/CEI 27001:2005, *Technologies de l'information — Techniques de sécurité — Systèmes de gestion de la sécurité de l'information — Exigences*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/CEI 27000 et les suivants s'appliquent.

NOTE Les différences de définitions entre l'ISO/CEI 27005:2008 et la présente Norme internationale sont indiquées dans l'Annexe G.

3.1
conséquence
effet d'un **événement** (3.3) affectant les objectifs

[Guide ISO 73:2009]

NOTE 1 Un événement unique peut engendrer des conséquences multiples.