NORME INTERNATIONALE

ISO/IEC 27006

Troisième édition
2015-10

Technologies de l'information — Techniques de sécurité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems

Numéro de référence
ISO/IEC 27006:2015(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
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 document. 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 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 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, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

L'ISO/IEC 27006 a été élaborée par le comité technique mixte ISO/IEC TC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

La présente troisième édition annule et remplace la deuxième édition (ISO/IEC 27006:2011) qui a fait l'objet d'une révision technique.

Introduction

L'ISO/IEC 17021-1 énonce les critères applicables aux organismes procédant à l'audit et à la certification des systèmes de management. Si lesdits organismes sont à accréditer comme étant conformes à l'ISO/IEC 17021-1 dans le but de procéder à l'audit et de certifier les systèmes de management de la sécurité de l'information (SMSI) conformément à l'ISO/IEC 27001:2013, certaines exigences et recommandations complémentaires de l'ISO/IEC 17021-1 sont nécessaires. Celles-ci sont fournies par la présente Norme internationale.

Le texte de la présente Norme internationale suit la structure de l'ISO/IEC 17021-1, et les exigences et recommandations spécifiques aux SMSI relatives à l'application de l'ISO/IEC 17021-1 pour la certification de SMSI sont identifiées par les lettres « SI ».

Le terme « shall » (doit) est utilisé dans la version en langue anglaise de la présente Norme internationale pour indiquer les dispositions qui, conformément aux exigences de l'ISO/IEC 17021-1 et de l'ISO/IEC 27001, revêtent un caractère obligatoire. Le terme « should » (il convient de/que) est utilisé pour indiquer une recommandation.

L'objectif principal de la présente Norme internationale est de permettre aux organismes d'accréditation d'harmoniser plus efficacement l'application des normes sur la base desquelles ils sont tenus d'évaluer les organismes de certification.

Dans l'ensemble de la présente Norme internationale, les termes « système de management » et « système » sont utilisés de façon interchangeable. La définition d'un système de management est disponible dans l'ISO 9000:2005. Le système de management utilisé dans la présente Norme internationale n'est pas à confondre avec d'autres types de systèmes, tels que les systèmes d'information.

