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)

© ISO/IEC 2015



DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2015

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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 ..... **v**
Introduction ..... **vi**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Principes **1**
5 Exigences générales **2**
5.1 Domaine juridique et contractuel 2
5.2 Gestion de l'impartialité 2
5.2.1 SI 5.2 Conflits d'intérêts 2
5.3 Responsabilité et situation financière 2
6 Exigences structurelles **2**
7 Exigences relatives aux ressources **2**
7.1 Compétence du personnel 2
7.1.1 SI 7.1.1 Considérations générales 3
7.1.2 SI 7.1.2 Détermination des critères de compétence 3
7.2 Personnel intervenant dans les activités de certification 7
7.2.1 SI 7.2 Démonstration des connaissances et de l'expérience des auditeurs 7
7.3 Intervention d'auditeurs et d'experts techniques externes individuels 8
7.3.1 SI 7.3 Intervention d'auditeurs externes ou d'experts techniques externes au sein de l'équipe d'audit 8
7.4 Enregistrements relatifs au personnel 8
7.5 Externalisation 8
8 Exigences relatives aux informations **8**
8.1 Informations publiques 8
8.2 Documents de certification 8
8.2.1 SI 8.2 Documents de certification SMSI 8
8.3 Référence à la certification et utilisation des marques 9
8.4 Confidentialité 9
8.4.1 SI 8.4 Accès aux enregistrements de l'organisation 9
8.5 Échange d'informations entre l'organisme de certification et ses clients 9
9 Exigences relatives aux processus **9**
9.1 Activités préalables à la certification 9
9.1.1 Demande de certification 9
9.1.2 Revue de la demande 9
9.1.3 Programme d'audit 9
9.1.4 Détermination du temps d'audit 10
9.1.5 Échantillonnage multisite 11
9.1.6 Systèmes de management multiples 12
9.2 Planification des audits 12
9.2.1 Détermination des objectifs, du domaine d'application et des critères de l'audit 12
9.2.2 Constitution de l'équipe d'audit et affectation des missions 12
9.2.3 Plan d'audit 13
9.3 Certification initiale 14
9.3.1 SI 9.3.1 Audit de certification initiale 14
9.4 Réalisation des audits 15
9.4.1 SI 9.4 Généralités 15
9.4.2 SI 9.4 Éléments spécifiques de l'audit de SMSI 15
9.4.3 SI 9.4 Rapport d'audit 15
9.5 Décision de certification 16

© ISO/IEC 2015 – Tous droits réservés

9.5.1 SI 9.5 Décision de certification ... 16
9.6 Maintien de la certification ... 16
9.6.1 Généralités ... 16
9.6.2 Activités de surveillance ... 16
9.6.3 Recertification ... 17
9.6.4 Audits particuliers ... 18
9.6.5 Suspension, retrait ou réduction du domaine d'application de la certification ... 18
9.7 Appels ... 18
9.8 Plaintes ... 18
9.8.1 SI 9.8 Plaintes ... 18
9.9 Enregistrements relatifs au client ... 18

10 Exigences relatives au système de management des organismes de certification ... 18
10.1 Options ... 18
10.1.1 SI 10.1 Mise en œuvre du SMSI ... 18
10.2 Option A : Exigences générales relatives au système de management ... 18
10.3 Option B : Exigences relatives au système de management conformément à l'ISO 9001 ... 18

Annexe A (informative) **Connaissances et savoir-faire requis pour l'audit et la certification d'un SMSI ... 19**

Annexe B (normative) **Temps d'audit ... 21**

Annexe C (informative) **Méthodes de calcul du temps d'audit ... 26**

Annexe D (informative) **Recommandations pour la revue des mesures mises en œuvre de l'Annexe A de l'ISO/IEC 27001:2013 ... 30**

Bibliographie ... 39

 © ISO/IEC 2015 – Tous droits réservés

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.

© ISO/IEC 2015 – Tous droits réservés

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.

 © ISO/IEC 2015 – Tous droits réservés

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

1 Domaine d'application

La présente Norme internationale spécifie les exigences et fournit des recommandations pour les organismes procédant à l'audit et à la certification d'un système de management de la sécurité de l'information (SMSI), en plus des exigences contenues dans l'ISO/IEC 17021-1 et l'ISO/IEC 27001. Elle a pour principal objet de soutenir l'accréditation des organismes de certification qui procèdent à la certification de SMSI.

Il est nécessaire que tout organisme qui procède à la certification de SMSI démontre qu'il respecte les exigences stipulées dans la présente Norme internationale en termes de compétences et de fiabilité, et les recommandations contenues dans la présente Norme internationale fournissent une interprétation supplémentaire de ces exigences pour tout organisme procédant à la certification de SMSI.

NOTE La présente Norme internationale peut être utilisée comme référentiel pour l'accréditation, l'évaluation par des pairs ou d'autres processus d'audit.

2 Références normatives

Les documents ci-après, dans leur intégralité ou non, sont des références normatives indispensables à 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/IEC 17021-1:2015, *Évaluation de la conformité — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management — Partie 1: Exigences*

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

ISO/IEC 27001:2013, *Technologies de l'information — Techniques de sécurité — Systèmes de management 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/IEC 17021-1, l'ISO/IEC 27000 et les suivants s'appliquent.

3.1
documents de certification
documents indiquant que le SMSI d'un client est conforme à des normes de SMSI spécifiées et à toute documentation supplémentaire requise en vertu du système

4 Principes

Les principes de l'ISO/IEC 17021-1, 4 s'appliquent.

© ISO/IEC 2015 – Tous droits réservés