NORME INTERNATIONALE

ISO/IEC 27006

Troisième édition
2015-10-01

AMENDEMENT 1
2020-03

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

AMENDEMENT 1

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

AMENDMENT 1

Numéro de référence
ISO/IEC 27006:2015/Amd.1:2020(F)

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

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.

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) ou dans la liste des déclarations de brevets reçues par l'IEC (voir https://patents.iec.c).

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 le lien suivant : www.iso.org/iso/foreword.html.

Le présent document a été élaboré par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

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/members.html.

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

AMENDEMENT 1

7.2.1.1 d)

Remplacer le texte par ce qui suit :

d) a acquis une expérience en matière d'audit de SMSI avant d'intervenir comme auditeur effectuant des audits de SMSI. Cette expérience doit être acquise par l'intervention comme auditeur en formation encadré par un évaluateur de SMSI (voir le paragraphe 9.2.2.1.4 de l'ISO/IEC 17021-1:2015) sur au moins un audit de certification initiale de SMSI (étape 1 et étape 2) ou une recertification et au moins un audit de surveillance. Cette expérience doit être acquise par au moins 10 jours d'audit sur site de SMSI au cours des 5 dernières années. Cette participation doit inclure la revue de la documentation et l'appréciation du risque, l'évaluation de la mise en œuvre et l'élaboration de rapports d'audit.

7.2.1.1

Ajouter un nouvel alinéa g) comme suit :

g) possède des compétences d'audit de SMSI conformément à l'ISO/IEC 27001.

8.2.1

Remplacer le dernier paragraphe par le texte suivant :

Les documents de certification peuvent faire référence à des normes nationales et internationales comme source(s) d'ensemble de mesures pour les mesures qui sont sélectionnés comme étant nécessaires dans la Déclaration d'applicabilité de l'organisation conformément au paragraphe 6.1.3 d) de l'ISO/IEC 27001:2013. Il faut indiquer de façon claire que cette référence sur les documents de certification représente uniquement une source d'ensemble de mesures pour les mesures sélectionnées dans la Déclaration d'applicabilité et non une certification de cette référence.

9.3.1.1

Remplacer le troisième paragraphe par le texte suivant :

Les résultats de l'étape 1 doivent être documentés dans un rapport écrit. L'organisme de certification doit passer en revue le rapport d'audit de l'étape 1 avant de décider de passer à l'étape 2 et doit confirmer si les membres de l'équipe d'audit de l'étape 2 possèdent les compétences nécessaires ; cela peut être effectué par l'auditeur responsable de l'équipe qui a effectuée l'audit d'étape 1 s'il est jugé compétent et si cela est approprié.

NOTE Une revue indépendante (c'est-à-dire par une personne de l'organisme de certification n'ayant pas participé à l'audit) est une mesure permettant d'atténuer les risques encourus lorsqu'il s'agit de décider de passer ou non à l'étape 2, et avec qui le faire. Cependant, d'autres mesures d'atténuation des risques peuvent déjà être en place et atteindre le même objectif.

B.2.1

Remplacer le premier paragraphe par le texte suivant :

Le nombre total de personnes effectuant un travail sous le contrôle de l'organisation pour tous les postes de travail inclus dans le domaine d'application de la certification constitue le point de départ de la détermination du temps d'audit.

B.3.6

Remplacer le premier paragraphe par le texte suivant :

Il est attendu que le temps calculé pour la combinaison de la planification et de la rédaction du rapport ne devrait généralement pas réduire le « temps d'audit » sur site total à moins de 70 % du temps calculé conformément aux paragraphes B.3.3 et B.3.4. Lorsqu'un temps supplémentaire est nécessaire pour la planification et/ou la rédaction du rapport, cela ne doit pas être un motif de réduction du temps d'audit sur site. Les temps de déplacement de l'auditeur ne sont pas inclus dans ce calcul et s'ajoutent au temps d'audit indiqué dans le tableau.

B.6

Remplacer le premier paragraphe par le texte suivant :

Le nombre total de jours d'audit sur site – tel que calculé pour le domaine d'application conformément à la procédure indiquée en B.3.3 – doit être réparti entre les différents sites sur la base de l'intérêt du site dans le système de management et des risques identifiés. La justification de la répartition doit être enregistrée par l'organisme de certification.

Le temps total consacré à l'audit initial et à la surveillance est la somme totale du temps passé sur chaque site ainsi qu'au siège social et il ne doit jamais être inférieur à celui qui aurait été calculé pour la taille et la complexité de l'exploitation si le travail avait intégralement été effectué sur un site unique (c'est-à-dire avec tous les employés de la société sur le même site).

ICS 35.030

Prix basé sur 2 pages