Norme internationale

ISO/IEC 27006-1

Première édition
2024-03

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information —

Partie 1: Généralités

Information security, cybersecurity and privacy protection — Requirements for bodies providing audit and certification of information security management systems —

Part 1: General

Numéro de référence
ISO/IEC 27006-1:2024(fr)

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.

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 ou www.iec.ch/members_experts/refdocs).

L'ISO et l'IEC attirent l'attention sur le fait que la mise en application du présent document peut entraîner l'utilisation d'un ou de plusieurs brevets. L'ISO et l'IEC ne prennent pas position quant à la preuve, à la validité et à l'applicabilité de tout droit de brevet revendiqué à cet égard. À la date de publication du présent document, L'ISO et l'IEC n'avaient pas reçu notification qu'un ou plusieurs brevets pouvaient être nécessaires à sa mise en application. Toutefois, il y a lieu d'avertir les responsables de la mise en application du présent document que des informations plus récentes sont susceptibles de figurer dans la base de données de brevets, disponible à l'adresse www.iso.org/brevets et https://patents.iec.ch. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié tout ou partie de tels droits de propriété.

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/iso/avant-propos. Pour l'IEC, voir www.iec.ch/understanding-standards.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée,* en collaboration avec le comité technique CEN/CLC/JTC 13, *Cybersécurité et protection des données*, du Comité européen de normalisation (CEN), conformément à l'Accord de coopération technique entre l'ISO et le CEN (Accord de Vienne).

Cette première édition de l'ISO/IEC 27006-1 annule et remplace l'ISO/IEC 27006:2015, qui a fait l'objet d'une révision technique. Elle incorpore également l'Amendement ISO/IEC 27006:2015/Amd 1:2020.

Les principales modifications sont les suivantes:

— le présent document a été converti en première partie d'une série en plusieurs parties;

— l'ensemble du document a été mis à jour pour les audits à distance et les organismes ayant peu ou pas de sites physiques pertinents;

— le concept de personnes effectuant certaines activités identiques a été introduit au point C.3.4 et plusieurs mises à jour ont été effectuées;

— le présent document (en particulier l'Annexe E) a été aligné sur l'ISO/IEC 27001:2022 et l'ISO/IEC 27002:2022;

— les redondances avec l'ISO/IEC 17021-1 ont été supprimées;

— la rédaction a été clarifié et plus étroitement alignée sur l'ISO/IEC 17021-1.

Une liste de toutes les parties de la série ISO/IEC 27006 se trouve sur les sites Web de l'ISO et de l'IEC.

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 et www.iec.ch/national-committees.

Introduction

L'ISO/IEC 17021-1 énonce des exigences et des recommandations applicables aux organismes procédant à l'audit et à la certification des systèmes de management. Si lesdits organismes entendent se conformer 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, certaines exigences et recommandations complémentaires de l'ISO/IEC 17021-1 sont nécessaires. Celles-ci sont fournies par le présent document.

Le présent document spécifie les exigences applicables aux organismes procédant à l'audit et à la certification d'un SMSI. Il énonce des exigences génériques pour ces organismes, appelés organismes de certification. Le respect de ces exigences a pour but de garantir que les organismes de certification procèdent à la certification des SMSI avec compétence, cohérence et impartialité, facilitant ainsi la reconnaissance de ces organismes et l'acceptation de leurs certifications à un niveau national et international.

Le texte du présent document respecte la structure de l'ISO/IEC 17021-1:2015.

Dans le présent document, les formes verbales suivantes sont utilisées:

— «doit» indique une exigence;

— «il convient» indique une recommandation;

— «peut» indique une autorisation («may» en anglais);

— «peut» indique une possibilité ou une capacité («can» en anglais).