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).

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**

1 Domaine d'application

Le présent document 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.

Les organismes qui procèdent à la certification de systèmes ISMS démontrent qu'ils respectent les exigences de compétence et de fiabilité présentées dans le présent document. Les recommandations contenues dans le présent document fournissent une interprétation supplémentaire de ces exigences pour les organismes procédant à la certification de systèmes ISMS.

NOTE Le présent document peut être utilisé comme référentiel pour l'accréditation, l'évaluation par des pairs ou d'autres processus d'audit.

2 Références normatives

Les documents suivants sont cités dans le texte de sorte qu'ils constituent, pour tout ou partie de leur contenu, des exigences 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 27001:2022, *Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la sécurité de l'information — Exigences*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions de l'ISO/IEC 17021-1 ainsi que les suivants s'appliquent.

L'ISO et l'IEC tiennent à jour des bases de données terminologiques destinées à être utilisées en normalisation, consultables aux adresses suivantes:

— ISO Online browsing platform: disponible à l'adresse https://www.iso.org/obp

— IEC Electropedia: disponible à l'adresse https://www.electropedia.org/

3.1
document de certification
document indiquant que le système de management de la sécurité de l'information (SMSI) d'un client est conforme à des normes de SMSI spécifiées et à toute documentation supplémentaire requise en vertu du système de management

Note 1 à l'article: La présente définition ne limite pas le nombre de documents collectivement appelés «documents de certification».

3.2
mesure de sécurité
action qui maintient et/ou modifie un *risque* (3.10)

Note 1 à l'article: Une mesure de sécurité du risque inclut, sans toutefois s'y limiter, n'importe quels processus, politiques, dispositifs, pratiques ou autres conditions et/ou actions qui maintiennent et/ou modifient un *risque* (3.10).

Note 2 à l'article: Une mesure de sécurité n'aboutit pas toujours nécessairement à la modification voulue ou supposée.

[SOURCE: ISO/IEC 27002:2022, 3.1.8]

3.3
contexte externe
environnement externe dans lequel l'*organisme* (3.9) cherche à atteindre ses objectifs

Note 1 à l'article: Le contexte externe peut inclure les aspects suivants:

— l'environnement culturel, social, politique, légal, réglementaire, financier, technologique, économique, naturel et concurrentiel, au niveau international, national, régional ou local;

— les facteurs clés et tendances ayant un impact déterminant sur les objectifs de l'*organisme* (3.9);

— les relations avec les parties prenantes externes, les perceptions et valeurs relatives à celles-ci.

[SOURCE: ISO/IEC 27000:2018, 3.22]

3.4
sécurité de l'information
protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

Note 1 à l'article: En outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation, et la fiabilité peuvent également être concernées.

[SOURCE: ISO/IEC 27000:2018, 3.28]

3.5
incident lié à la sécurité de l'information
un ou plusieurs événements liés à la sécurité de l'information, indésirables ou inattendus, présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la *sécurité de l'information* (3.4)

[SOURCE: ISO/IEC 27000:2018, 3.31]

3.6
système d'information
ensemble d'applications, services, actifs informationnels ou autres composants permettant de gérer l'information

[SOURCE: ISO/IEC 27000:2018, 3.35]

3.7
contexte interne
environnement interne dans lequel l'*organisme* (3.9) cherche à atteindre ses objectifs

Note 1 à l'article: Le contexte interne peut inclure:

— la gouvernance, la structure organisationnelle, les rôles et les responsabilités;

— les politiques, objectifs et stratégies mises en place pour atteindre ces derniers;

— les capacités, en termes de ressources et de connaissances (par exemple: capital, temps, personnel, processus, systèmes et technologies);

— *les systèmes d'information* (3.6), flux d'information et processus de prise de décision (formels et informels);

— les relations avec les parties prenantes internes, les perceptions et valeurs associées à celles-ci;

— la culture de l'*organisme* (3.9);

— les normes, lignes directrices et modèles adoptés par l'*organisme* (3.9);

— la forme et l'étendue des relations contractuelles.

[SOURCE: ISO/IEC 27000:2018, 3.38]

3.8
système de management
ensemble d'éléments corrélés ou en interaction d'un *organisme* (3.9), utilisés pour établir des politiques, des objectifs et des processus de façon à atteindre lesdits objectifs

Note 1 à l'article: Un système de management peut traiter d'un seul ou de plusieurs domaines, par exemple management de la qualité, gestion financière ou management environnemental.

Note 2 à l'article: Les éléments du système de management comprennent la structure, les rôles et responsabilités, la planification, le fonctionnement de l'*organisme* (3.9), les politiques, les pratiques, les règles, les convictions, les objectifs et les processus permettant d'atteindre ces objectifs.

Note 3 à l'article: Le périmètre d'un système de management peut comprendre l'ensemble de l'*organisme* (3.9), des fonctions ou des sections spécifiques et identifiées de l'*organisme* (3.9), ou une ou plusieurs fonctions dans un groupe d'*organismes* (3.9).

Note 4 à l'article: Il s'agit de l'un des termes communs et définitions de base pour les normes de systèmes de management de l'ISO, donnés dans l'Annexe SL du Supplément ISO consolidé aux Directives ISO/IEC, Partie 1. La définition initiale a fait l'objet d'une modification des Notes 1 à 3 à l'article.

[SOURCE: ISO 9000:2015, 3.5.3]

3.9
organisme
personne ou groupe de personnes qui exerce ses propres fonctions associées aux responsabilités, pouvoirs et relations nécessaires pour atteindre ses objectifs

Note 1 à l'article: Le concept d'organisme inclut, sans s'y limiter, les travailleurs indépendants, compagnies, sociétés, firmes, entreprises, autorités, partenariats, œuvres de bienfaisance ou institutions, ou toute partie ou combinaison de ceux-ci, constituée en société de capitaux ou ayant un autre statut, de droit privé ou public.

[SOURCE: ISO/IEC 27000:2018, 3.50]

3.10
risque
effet de l'incertitude sur les objectifs

Note 1 à l'article: Un effet est un écart, positif ou négatif, par rapport à une attente.

Note 2 à l'article: L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

Note 3 à l'article: Un risque est souvent caractérisé en référence à des «événements» potentiels (tels que définis dans le Guide ISO 73:2009, 3.5.1.3) et à des «conséquences» potentielles (telles que définies dans le Guide ISO 73:2009, 3.6.1.3), ou à une combinaison des deux.

Note 4 à l'article: Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa «vraisemblance» (telle que définie dans le Guide ISO 73:2009, 3.6.1.1).

Note 5 à l'article: Dans le contexte des systèmes de management de la sécurité de l'information, les risques liés à la sécurité de l'information peuvent être exprimés comme l'effet de l'incertitude sur les objectifs de sécurité de l'information.

Note 6 à l'article: Le risque lié à la sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités d'un actif ou d'un groupe d'actifs informationnels et nuisent donc à un *organisme* (3.9).

[SOURCE: ISO/IEC 27000:2018, 3.61]

3.11
analyse du risque
processus mis en œuvre pour comprendre la nature d'un *risque* (3.10) et pour déterminer le niveau de risque

Note 1 à l'article: L'analyse du risque fournit la base de l'évaluation du risque et des décisions relatives au *traitement du risque* (3.14).

Note 2 à l'article: L'analyse du risque inclut l'estimation du risque.

[SOURCE: ISO/IEC 27000:2018, 3.63]

3.12
appréciation du risque
ensemble du processus d'identification du risque, d'*analyse du risque* (3.11) et d'évaluation du risque

[SOURCE: ISO/IEC 27000:2018, 3.64]

3.13
gestion des risques
activités coordonnées visant à diriger et contrôler un *organisme* (3.9) vis-à-vis du *risque* (3.10)

[SOURCE: ISO/IEC 27000:2018, 3.69]

3.14
traitement du risque
processus destiné à modifier un *risque* (3.10)

Note 1 à l'article: Le traitement du risque peut inclure:

— un refus du risque en décidant de ne pas démarrer ni poursuivre l'activité porteuse du risque;

— la prise ou l'augmentation d'un risque afin de saisir une opportunité;

— l'élimination de la source de risque;

— une modification de la vraisemblance;

— une modification des conséquences;

— un partage du risque avec une ou plusieurs autres parties (incluant des contrats et un financement du risque);

— un maintien du risque fondé sur un choix argumenté.

Note 2 à l'article: Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque».

Note 3 à l'article: Le traitement du risque peut créer de nouveaux risques ou modifier des *risques* (3.10) existants.

[SOURCE: ISO/IEC 27000:2018, 3.72]

3.15
règle
principe admis ou instruction formulant les attentes de l'*organisation* (3.9) sur ce qui est nécessaire de faire, ce qui est autorisé ou ce qui ne l'est pas

[SOURCE: ISO/IEC 27002:2022, 3.1.32 — modifié, la Note 1 à l'article a été supprimée.]

4 Principes

Les principes de l'ISO/IEC 17021-1:2015, Article 4 doivent s'appliquer.

5 Exigences générales

5.1 Domaine juridique et contractuel

Les exigences de l'ISO/IEC 17021-1:2015, 5.1, doivent s'appliquer.

5.2 Gestion de l'impartialité

5.2.1 Généralités

Les exigences de l'ISO/IEC 17021-1:2015, 5.2, doivent s'appliquer. De plus, les exigences et recommandations énoncées au 5.2.2 doivent s'appliquer.

5.2.2 Conflits d'intérêts

Les organismes de certification peuvent apporter une valeur ajoutée lors des audits de certification et de surveillance (par exemple en identifiant les opportunités d'amélioration au fur et à mesure qu'elles apparaissent au cours de l'audit, sans recommander de solutions spécifiques) sans que celles-ci soient considérées comme des activités de conseil ou qu'elles génèrent un potentiel conflit d'intérêts.

L'organisme de certification ne doit pas fournir de revues internes de la sécurité de l'information du SMSI du client soumis à certification. De plus, l'organisme de certification doit être indépendant du ou des organismes (y compris de toutes personnes) qui effectuent l'audit interne du SMSI.

5.3 Responsabilité et situation financière

Les exigences de l'ISO/IEC 17021-1:2015, 5.3, doivent s'appliquer.

6 Exigences structurelles

Les exigences spécifiées dans l'ISO/IEC 17021-1:2015, Article 6, doivent s'appliquer.

7 Exigences relatives aux ressources

7.1 Compétence du personnel

7.1.1 Généralités

Les exigences de l'ISO/IEC 17021-1:2015, 7.1, doivent s'appliquer. De plus, les exigences et recommandations énoncées aux paragraphes 7.1.2 et 7.1.3 doivent s'appliquer.

7.1.2 Exigences génériques en matière de compétence

L'organisme de certification doit définir les exigences en matière de compétence pour chaque fonction de certification référencée dans l'ISO/IEC 17021-1:2015, Tableau A.1. L'organisme de certification doit prendre en compte l'ensemble des exigences spécifiées dans l'ISO/IEC 17021-1 et les paragraphes 7.1.3 et 7.2.2 du présent document qui sont pertinents pour les secteurs techniques du SMSI tel que déterminé par l'organisme de certification. L'Annexe B fournit d'autres guides sur les compétences.

L'organisme de certification doit définir les connaissances et les compétences requises pour certaines fonctions conformément à l'Annexe A.

Lorsque des critères spécifiques supplémentaires, y compris des exigences en matière de compétences, ont été établis dans une norme spécifique (par exemple ISO/IEC 27006-2), ils doivent être appliqués.

7.1.3 Détermination des critères de compétence

7.1.3.1 Exigences de compétence pour l'audit de SMSI

7.1.3.1.1 Exigences générales

L'organisme de certification doit avoir mis en place des critères permettant de vérifier la compétence des membres de l'équipe d'audit afin de s'assurer qu'ils possèdent au moins les compétences nécessaires pour mettre en œuvre leurs connaissances dans les domaines suivants:

a) la sécurité de l'information;

b) les aspects techniques de l'activité à auditer;

c) les systèmes de management;

d) les principes de l'audit;

NOTE Des informations supplémentaires sur les principes de l'audit peuvent être trouvées dans l'ISO 19011.

e) la surveillance, la mesure, l'analyse et l'évaluation des SMSI.

Les exigences a) à e) ci-dessus s'appliquent à tous les auditeurs qui font partie de l'équipe d'audit. Toutefois, le point b) peut être partagé entre les membres de l'équipe d'audit.

L'équipe d'audit doit, collectivement, avoir les compétences nécessaires pour répondre aux exigences susmentionnées, ce qui peut être démontré par l'expérience de leur application.

L'équipe d'audit doit, collectivement, avoir les compétences lui permettant d'établir le lien entre les traces d'incidents de sécurité de l'information dans le SMSI du client et les éléments appropriés du SMSI.

Les auditeurs individuels ne sont pas tenus d'avoir un éventail complet d'expériences dans tous les domaines de la sécurité de l'information, mais l'équipe d'audit dans son ensemble doit posséder les compétences nécessaires pour couvrir le domaine d'application du SMSI soumis à l'audit.

7.1.3.1.2 Terminologie, principes, pratiques et techniques du management de la sécurité de l'information

Chaque auditeur d'une équipe d'audit de SMSI doit avoir connaissance:

a) des structures, de la hiérarchie de la documentation spécifique aux SMSI et des relations entre les documents;

b) de l'appréciation du risque et gestion des risques liés à la sécurité de l'information;

c) des processus applicables aux SMSI.