PROJET FINAL
Norme internationale

ISO/IEC FDIS 27706

Technologie 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 protection de la vie privée

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

ISO/IEC JTC **1**/SC **27**

Secrétariat: **DIN**

Début de vote:
2024-12-27

Vote clos le:
2025-02-21

LES DESTINATAIRES DU PRÉSENT PROJET SONT INVITÉS À PRÉSENTER, AVEC LEURS OBSERVATIONS, NOTIFICATION DES DROITS DE PROPRIÉTÉ DONT ILS AURAIENT ÉVENTUELLEMENT CONNAISSANCE ET À FOURNIR UNE DOCUMENTATION EXPLICATIVE.

OUTRE LE FAIT D'ÊTRE EXAMINÉS POUR ÉTABLIR S'ILS SONT ACCEPTABLES À DES FINS INDUSTRIELLES, TECHNOLOGIQUES ET COM-MERCIALES, AINSI QUE DU POINT DE VUE DES UTILISATEURS, LES PROJETS DE NORMES INTERNATIONALES DOIVENT PARFOIS ÊTRE CONSIDÉRÉS DU POINT DE VUE DE LEUR POSSIBILITÉ DE DEVENIR DES NORMES POUVANT SERVIR DE RÉFÉRENCE DANS LA RÉGLEMENTATION NATIONALE.

TRAITEMENT PARALLÈLE ISO/CEN

Numéro de référence
ISO/IEC FDIS 27706:2024(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 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 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 propriété 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 annule et remplace l'ISO/IEC TS 27006-2:2021 qui a fait l'objet d'une révision technique.

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 aux adresses www.iso.org/fr/members.html et www.iec.ch/national-committees.

Introduction

Le présent document définit les exigences applicables aux organismes assurant l'audit et la certification des systèmes de management de la protection de la vie privée conformément à l' ISO/IEC 27701.

Le présent document vise également à aider les organismes d'accréditation et les pairs évaluateurs à être en mesure d'évaluer les exigences minimales relatives à la compétence du personnel dans les organismes de certification et les processus de certification dans ces organismes de certification de manière efficace et harmonisée.

Technologie 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 protection de la vie privée

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 des systèmes de management de la protection de la vie privée (SMVP) conformément à l'ISO/IEC 27701, en complément des exigences contenues dans l'ISO/IEC 17021-1.

Les organismes qui procèdent à la certification de systèmes PIMS 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 PIMS.

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 17000, *Évaluation de la conformité — Vocabulaire et principes généraux*

ISO/IEC 17021-1, *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 27701:—[1)], *Sécurité de l'information, cybersécurité et protection de la vie privée — Systèmes de management de la protection de la vie privée — Exigences et recommandations*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO/IEC 17000, de l'ISO/IEC 17021-1, et de l'ISO/IEC 27701, 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/

1) En cours d'élaboration. Stade à la date de publication: ISO/IEC DIS 27701:2024.

3.1
document de certification
document indiquant que le système de management de la protection de la vie privée d'un client est conforme à l'ISO/IEC 27701 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».

[SOURCE: ISO/IEC 27006-1:2024, 3.1, modifié — les références au «système de management de la sécurité de l'information» ont été modifiées en «système de management de la protection de la vie privée» et la référence à l'ISO/IEC 27001 a été remplacée par l'ISO/IEC 27701.]

3.2
données à caractère personnel
DCP
information qui (a) peut être utilisée pour établir un lien entre les informations et la personne physique à laquelle ces informations se rapportent, ou qui (b) est ou peut être directement ou indirectement associée à une personne physique

Note 1 à l'article: La «personne physique» référencée dans la définition est la *personne concernée* (3.4). Pour déterminer si une personne concernée est identifiable, il convient de tenir compte de tous les moyens pouvant être raisonnablement utilisés par la partie prenante en matière de protection de la vie privée qui détient les données, ou par toute autre partie, afin d'établir le lien entre l'ensemble de DCP et la personne physique.

[SOURCE: ISO/IEC 29100:2024, 3.7]

3.3
responsable de traitement de DCP
partie(s) prenante(s) du domaine de la vie privée qui détermine(-nt) la fin et les moyens pour le traitement d'*informations personnelles identifiables (PII)* (3.2) autre(s) que les personnes physiques qui utilisent des données à des fins personnelles

Note 1 à l'article: Un responsable de traitement de DCP demande parfois à des tiers [par exemple, des *sous-traitants de DCP* (3.5)] de *traiter des DCP* (3.8) en son nom, bien qu'un tel traitement relève toujours de la responsabilité du responsable de traitement de DCP.

[SOURCE: ISO/IEC 29100:2024, 3.8]

3.4
personne concernée
sujet des données
personne physique à qui se rapportent les *informations personnelles identifiables (PII)* (3.2)

[SOURCE: ISO/IEC 29100:2024, 3.9]

3.5
sous-traitant de DCP
partie prenante du domaine de la vie privée qui traite des *informations personnelles identifiables (PII)* (3.2) pour le compte d'un *contrôleur de PII* (3.3) et conformément à ses instructions

[SOURCE: ISO/IEC 29100:2024, 3.10]

3.6
système de management de la protection de la vie privée
SMVP
système de management qui gère la protection de la vie privée telle que potentiellement affectée par le *traitement des DCP* (3.8)

[SOURCE: ISO/IEC 27701:—, 3.23]

3.7
évaluation de l'impact sur la vie privée
évaluation des risques sur la vie privée
processus global visant à identifier, analyser, évaluer, consulter, communiquer et planifier le traitement des impacts potentiels sur la vie privée au regard du traitement des *données à caractère personnel* (3.2), dans le cadre plus large du système de management des risques d'un organisme

[SOURCE: ISO/IEC 29100:2024, 3.18]

3.8
traitement de DCP
opération ou ensemble d'opérations exécutées sur des *données à caractère personnel (DCP)* (3.7)

Note 1 à l'article: Les opérations de traitement des DCP incluent par exemple, sans toutefois s'y limiter, la collecte, le stockage, l'altération, la récupération, la consultation, la divulgation, l'anonymisation, la pseudonymisation, la distribution ou toute autre mise à disposition, la suppression ou la destruction de DCP.

[SOURCE: ISO/IEC 29100: 2024, 3.21]

3.9
déclaration d'applicabilité
documentation de toutes les mesures de sécurité nécessaires et justification de l'inclusion ou de l'exclusion de telles mesures

[SOURCE: ISO/IEC 27701:—, 3.25]

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 Considérations générales

Les exigences de l'ISO/IEC 17021-1:2015, 5.2 doivent s'appliquer.

5.2.2 Conflits d'intérêts

Outre les exigences de l'ISO/IEC 17021-1:2015, 5.2.5, les organismes de certification ne doivent pas fournir de prestations de conseil relatives aux systèmes de management liés à la protection de la vie privée, à la protection des données (par exemple sous la forme d'un délégué à la protection des données externe ou d'un contrôle de la protection des données) ou à la gestion des risques d'atteinte à la vie privée.

Les organismes de certification peuvent effectuer les activités suivantes sans que celles-ci soient considérées comme des activités de conseil ou qu'elles génèrent un potentiel conflit d'intérêts:

a) fournir uniquement des informations génériques et accessibles au public lors de l'organisation et de la participation en tant que conférencier à des cours de formation relatifs aux systèmes de management de la protection de la vie privée, aux systèmes de management ou à l'audit;

b) apporter de la plus-value pendant les audits de certification et de surveillance, par exemple en identifiant des opportunités d'amélioration, lorsqu'elles apparaissent pendant l'audit.

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 de l'ISO/IEC 17021-1:2015, Article 6 doivent s'appliquer.

7 Exigences relatives aux ressources

7.1 Compétence du personnel

7.1.1 Considérations générales

Les exigences de l'ISO/IEC 17021-1:2015, 7.1.1 doivent s'appliquer.

7.1.2 Détermination des critères de compétence

7.1.2.1 Généralités

Les exigences de l'ISO/IEC 17021-1:2015, 7.1.2 doivent s'appliquer.

7.1.2.2 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 également tenir compte des exigences spécifiées à l'Annexe C, pour les domaines techniques du SMVP.

L'organisme de certification doit prendre en compte les exigences de compétence d'une équipe d'audit en matière de sécurité de l'information conformément aux exigences de l'ISO/IEC 27701.

NOTE L'ISO/IEC 27006-1:2024, 7.1.3 fournit des exigences de compétence en matière de sécurité de l'information.

7.1.3 Processus d'évaluation

7.1.3.1 Généralités

Les exigences de l'ISO/IEC 17021-1:2015, 7.1.3 doivent s'appliquer.

7.1.3.2 Évaluation des auditeurs

L'organisme de certification doit démontrer que les auditeurs possèdent les connaissances et l'expérience nécessaires par au moins l'un des moyens suivants:

a) des qualifications reconnues spécifiques aux SMVP;

b) la participation à des formations sur les SMVP et l'obtention de qualifications personnelles pertinentes;

c) des enregistrements de perfectionnement professionnel à jour;

d) la réalisation d'audits de SMVP supervisés par un autre auditeur de SMVP compétent et qualifié.

NOTE Les connaissances et compétences dans le domaine de la protection de la vie privée peuvent inclure la réalisation d'audits de SMVP sous le contrôle d'autres auditeurs de SMVP qualifiés, ainsi que des connaissances et compétences spécifiques aux systèmes de management de la protection de la vie privée.

7.1.3.3 Sélection des auditeurs

Outre les exigences du paragraphe 7.1.3.1, le processus de sélection des auditeurs doit assurer que chaque auditeur:

a) possède une expérience professionnelle dans le domaine de la protection de la vie privée pour assurer le rôle d'auditeur pour les SMVP;

b) a reçu une formation dans le domaine de l'audit de SMVP et de management des audits, et a démontré ses compétences à réaliser des audits de SMVP conformément à l'ISO/IEC 27701;

c) maintient à jour et adapte ses connaissances et ses compétences dans le domaine du management de la protection de la vie privée et de l'audit à travers un perfectionnement professionnel continu.

7.1.3.4 Sélection des experts techniques

Le processus de sélection d'experts techniques doit assurer que chaque expert technique:

a) possède une expérience professionnelle dans le domaine de la protection de la vie privée pour assurer le rôle d'expert technique;

b) maintient à jour et adapte ses connaissances et ses compétences dans le domaine du management de la protection de la vie privée à travers un perfectionnement professionnel continu.

7.1.4 Autres considérations

Les exigences de l'ISO/IEC 17021-1:2015, 7.1.4 doivent s'appliquer.

7.2 Personnel intervenant dans les activités de certification

Les exigences de l'ISO/IEC 17021-1:2015, 7.2 doivent s'appliquer.

7.3 Intervention d'auditeurs et d'experts techniques externes individuels

Les exigences de l'ISO/IEC 17021-1:2015, 7.3 doivent s'appliquer.

7.4 Enregistrements relatifs au personnel

Les exigences de l'ISO/IEC 17021-1:2015, 7.4 doivent s'appliquer.

7.5 Externalisation

Les exigences de l'ISO/IEC 17021-1:2015, 7.5 doivent s'appliquer.

8 Exigences relatives aux informations

8.1 Informations publiques

Les exigences de l'ISO/IEC 17021-1-2015, 8.1 doivent s'appliquer.

8.2 Documents de certification

8.2.1 Généralités

Les exigences de l'ISO/IEC 17021-1-2015, 8.2 doivent s'appliquer.