Norme internationale

ISO/IEC 19896-3

Deuxième édition
2025-11

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences relatives aux compétences du personnel des organismes d'évaluation de la conformité de la sécurité TI —

Partie 3: Exigences en matière de connaissances et de compétences pour les évaluateurs et les examinateurs conformément à la série ISO/IEC 15408 et à l'ISO/IEC 18045

Information security, cybersecurity and privacy protection — Requirements for the competence of IT security conformance assessment body personnel —

Part 3: Knowledge and skills requirements for evaluators and reviewers according to the ISO/IEC 15408 series and ISO/IEC 18045

Numéro de référence
ISO/IEC 19896-3:2025(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. 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 deuxième édition annule et remplace la première édition (ISO/IEC 19896-2:2018), qui fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— les exigences pour les évaluateurs ont été entièrement retravaillées, y compris la restructuration du contenu;

— des exigences ont été ajoutées pour le personnel chargé d'examiner les activités d'évaluation de la conformité de la sécurité TI.

Une liste de toutes les parties de la série ISO/IEC 19896 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

La série ISO/IEC 15408 permet la comparaison entre des résultats d'évaluations de sécurité indépendantes. À cet effet, elle propose un ensemble commun d'exigences applicables aux fonctionnalités de sécurité des produits de technologies de l'information (TI) et aux mesures d'assurance appliquées à ces produits TI au cours d'une évaluation de sécurité. De nombreux schémas d'examen et d'évaluation ainsi que des organismes d'examen ont été élaborés en utilisant la série ISO/IEC 15408 et l'ISO/IEC 18045 comme base, ce qui permet de comparer les résultats des projets d'évaluation.

Le processus d'évaluation repose généralement à la fois sur des tests/méthodes prédéfinis pour un type de TOE et sur des tests/méthodes spécifiques à la TOE qui sont définis pour une implémentation donnée de la TOE. Par conséquent, la compétence des différents évaluateurs, dont il est attendu non seulement qu'ils appliquent les tests/méthodes prédéfinis, mais également qu'ils définissent et exécutent des tests/méthodes spécifiques à la TOE, est essentielle pour assurer la comparabilité et la répétabilité des résultats d'évaluation qui constituent le fondement de la reconnaissance mutuelle.

Le présent document établit une base de référence pour les compétences minimales des évaluateurs et examinateurs de la série ISO/IEC 15408 afin d'assurer l'harmonisation des exigences de formation des évaluateurs et examinateurs de l'ISO/IEC 15408. Il fournit des exigences spécialisées permettant aux personnes effectuant des évaluations et des examens de la sécurité des produits TI de démontrer leur compétence conformément à la série ISO/IEC 15408 et à l'ISO/IEC 18045. L'ISO/IEC 15408-1 décrit le cadre général des compétences, y compris les différents éléments de la compétence: connaissances, savoir-faire, expérience et instruction. Le présent document couvre notamment les connaissances et les savoir-faire dans les domaines suivants.

— Sécurité de l'information

  — Connaissances: principes de sécurité de l'information, propriétés de sécurité de l'information, menace et vulnérabilités en matière de sécurité de l'information.

  — Savoir-faire: compréhension des exigences en matière de sécurité de l'information, du contexte et du domaine d'application de l'évaluation.

— Évaluation de la sécurité de l'information

  — Connaissances: connaissance de la série ISO/IEC 15408 et de l'ISO/IEC 18045, système de management de laboratoire.

  — Savoir-faire: Savoir-faire de base en matière d'évaluation, savoir-faire essentiels en matière d'évaluation, savoir-faire requis lors de l'évaluation de classes d'assurance de la sécurité spécifiques, savoir-faire requis lors de l'évaluation de classes d'exigences fonctionnelles de sécurité spécifiques

— Architecture des systèmes d'information

  — Connaissances: technologie évaluée.

  — Savoir-faire: compréhension de l'interaction entre les composants de sécurité et les informations.

— Tests de sécurité de l'information

  — Connaissances: techniques de test de la sécurité de l'information, outils de test de la sécurité de l'information, cycle de vie du développement des produits, types de tests.

  — Savoir-faire: création et gestion d'un plan de test de sécurité de l'information, conception des tests de sécurité de l'information, préparation et réalisation des tests de sécurité de l'information.

Le public visé par le présent document comprend les organismes de certification des laboratoires de test, les organismes implémentant les schémas d'évaluation, les laboratoires, les évaluateurs et les organismes proposant des certifications professionnelles.

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences relatives aux compétences du personnel des organismes d'évaluation de la conformité de la sécurité TI —

Partie 3:
Exigences en matière de connaissances et de compétences pour les évaluateurs et les examinateurs conformément à la série ISO/IEC 15408 et à l'ISO/IEC 18045

1 Domaine d'application

Le présent document fournit les exigences spécialisées permettant aux personnes de démontrer leur compétence dans la réalisation d'évaluations et d'examens de la sécurité des produits TI conformément à la série ISO/IEC 15408 et à l'ISO/IEC 18045.

NOTE Il est possible que les évaluateurs et les testeurs appartiennent à des organismes opérant sous l'ISO/IEC 17025 et que les examinateurs appartiennent à des organismes opérant sous l'ISO/IEC 17065.

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 19896-1, *Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences relatives aux compétences du personnel des organismes d'évaluation de la conformité de la sécurité TI — Partie 1: Vue d'ensemble et concepts*

ISO/IEC 15408-1:—[1)], *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 1: Introduction et modèle général*

ISO/IEC 15408-2:—[2)], *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 2: Composants fonctionnels de sécurité*

ISO/IEC 15408-3:—[3)], *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 3: Composants d'assurance de sécurité*

ISO/IEC 15408-4, *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 4: Cadre prévu pour la spécification des méthodes d'évaluation et des activités connexes*

ISO/IEC 15408-5, *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 5: Paquets prédéfinis d'exigences de sécurité*

1) En cours d'élaboration. Stade à la date de publication: ISO/IEC FDIS 15408-1:2025.

2) En cours d'élaboration. Stade à la date de publication: ISO/IEC DIS 15408-2:2025.

3) En cours d'élaboration. Stade à la date de publication: ISO/IEC DIS 15408-3:2025.