Norme internationale

ISO/IEC 15408-4

Deuxième édition
2026-05

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 de spécification de méthodes et activités d'évaluation

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 4: Framework for the specification of evaluation methods and activities

Numéro de référence
ISO/IEC 15408-4:2026(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 mixte 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 15408-4:2022), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— correction d'erreurs typographiques et rédactionnelles mineures.

Une liste de toutes les parties de la série ISO/IEC 15408 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

Le modèle d'évaluation de la sécurité dans l'ISO/IEC 15408-1 indique que des activités d'évaluation génériques de haut niveau sont définies dans l'ISO/IEC 18045, mais que des activités d'évaluation (EA) plus spécifiques peuvent être définies comme des adaptations technologiques spécifiques de ces activités génériques pour des contextes d'évaluation particuliers, par exemple pour des exigences fonctionnelles de sécurité (SFR) ou des exigences d'assurance de sécurité (SAR) appliquées à des technologies spécifiques ou à certains types de cibles d'évaluation (TOE). La spécification de ces activités d'évaluation est déjà en cours chez les praticiens, ce qui crée un besoin de spécification pour la définition de ces activités d'évaluation.

Le présent document décrit un cadre qui peut être utilisé pour obtenir des activités d'évaluation à partir des unités de travail de l'ISO/IEC 18045 et pour les regrouper en méthodes d'évaluation (EM). Les activités ou méthodes d'évaluation peuvent être incluses dans les profils de protection (PP) et dans tout document les étayant. Lorsqu'un PP, une configuration de PP, un module de PP, un paquet ou une cible de sécurité (ST) indique que des méthodes/activités d'évaluation spécifiques doivent être utilisées, les évaluateurs sont tenus, par l'ISO/IEC 18045, de suivre et de rapporter les méthodes/activités d'évaluation pertinentes lors de l'attribution des verdicts. Comme indiqué dans l'ISO/IEC 15408-1, dans certains cas, une autorité d'évaluation peut décider de ne pas approuver l'utilisation de méthodes/activités d'évaluation particulières. Dans ce cas, l'autorité d'évaluation peut décider de ne pas effectuer d'évaluations à la suite d'une ST qui exige ces méthodes d'évaluation/activités d'évaluation.

Le présent document permet également de définir des activités d'évaluation pour les SAR étendues, auquel cas la dérivation des activités d'évaluation se rapporte aux éléments d'action de l'évaluateur et aux unités de travail équivalents définis pour cette SAR étendue. Lorsqu'il est fait référence dans le présent document à l'utilisation de l'ISO/IEC 18045 ou de l'ISO/IEC 15408-3 pour les SAR (par exemple lorsque l'on définit les argumentaires pour les activités d'évaluation), alors dans le cas d'une SAR étendue, la référence s'applique aux éléments d'action de l'évaluateur et aux unités de travail équivalentes définies pour cette SAR étendue.

Par souci de clarté, le présent document précise comment définir les méthodes et les activités d'évaluation, mais ne décrit pas lui-même des exemples de méthodes ou d'activités d'évaluation.

Plusieurs organisations gouvernementales ont contribué à l'élaboration de la présente version des critères communs pour la sécurité des technologies de l'information. Par la présente, en tant que cotitulaires des droits d'auteur des critères communs pour la sécurité des technologies de l'information (en abrégé, CC), ces organisations accordent à l'ISO/IEC une licence non exclusive d'utilisation des CC pour poursuivre l'élaboration/la maintenance de la série de normes ISO/IEC 15408. Toutefois, lesdites organisations gouvernementales se réservent le droit d'utiliser, de copier, de diffuser, de traduire ou de modifier les CC comme elles l'entendent. De plus amples informations concernant ces agences sont disponibles à l'adresse https://commoncriteriaportal.org/cc/copyright/index.cfm.

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 de spécification de méthodes et activités d'évaluation

1 Domaine d'application

Le présent document spécifie les exigences, ainsi qu'un cadre normalisé pour la spécification de méthodes d'évaluation et d'activités d'évaluation objectives, répétables et reproductibles.

Le présent document ne précise pas comment évaluer, adopter ou maintenir les méthodes et les activités d'évaluation. Ces aspects relèvent de la compétence de ceux qui sont à l'origine des méthodes et des activités d'évaluation dans leur domaine d'intérêt particulier.

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 15408-1, *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation de la sécurité informatique — Partie 1: Introduction et modèle général*

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

ISO/IEC 15408-3:2026, *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation de la sécurité informatique — Partie 3: Composants d'assurance de sécurité*

ISO/IEC 18045:2026, *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation de la sécurité informatique — Méthodologie d'évaluation de la sécurité informatique*

3 Termes, définitions et abréviations

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 15408-1, l'ISO/IEC 15408-2, l'ISO/IEC 15408-3, et l'ISO/IEC 18045 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/