Norme internationale

ISO/IEC 15408-3

Cinquième 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 3: Composants d'assurance de sécurité

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

Part 3: Security assurance components

Numéro de référence
ISO/IEC 15408-3:2026(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 cinquième édition annule et remplace la quatrième édition (ISO/IEC 15408-3:2022), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— la terminologie a été revue et mise à jour;

— un élément d'action de développeur manquant a été ajouté (ADV_SPM.1.7D).

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

Les composants d'assurance de sécurité, tels que définis dans le présent document, constituent la base des exigences d'assurance de sécurité exprimées dans un paquet d'assurance de sécurité, un profil de protection (PP), un module de PP, une configuration de PP ou une cible de sécurité (ST).

Ces exigences établissent une façon normalisée d'exprimer les exigences d'assurance des TOE. Le présent document propose un catalogue de l'ensemble des composants, des familles et des classes d'assurance. Il définit également des critères d'évaluation pour les PP, les configurations de PP, les modules de PP et les ST.

Il s'adresse notamment aux consommateurs, aux développeurs, aux groupes de travail techniques, aux évaluateurs de produits TI sécurisés. L'ISO/IEC 15408-1 fournit des informations supplémentaires sur le public cible de la série ISO/IEC 15408 et sur l'utilisation de la série ISO/IEC 15408 par les groupes qui composent le public cible. Les groupes suivants peuvent utiliser le présent document comme suit:

— les consommateurs qui utilisent le présent document lorsqu'ils choisissent des composants pour exprimer des exigences d'assurance afin de satisfaire aux objectifs de sécurité exprimés dans un PP ou une ST, déterminant les niveaux requis d'assurance de sécurité de la TOE;

— les développeurs, qui répondent aux exigences de sécurité des consommateurs réelles ou perçues lors de la construction d'une TOE, font référence au présent document lorsqu'ils interprètent les énoncés des exigences d'assurance et déterminent les approches d'assurance des TOE;

— les évaluateurs qui utilisent les exigences d'assurance définies dans le présent document comme un énoncé obligatoire des critères d'évaluation lors de la détermination de l'assurance des TOE et lors de l'évaluation des PP et des ST.

Dans le présent document, les caractères gras sont utilisés pour mettre en évidence les relations hiérarchiques entre les exigences. Cette convention d'écriture impose les caractères gras à toute nouvelle exigence.

Pour les exigences d'assurance de sécurité, les verbes spéciaux relatifs aux activités d'évaluation obligatoires sont présentés en caractères gras italiques.

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 3:
Composants d'assurance de sécurité

1 Domaine d'application

Le présent document spécifie les exigences d'assurance de sécurité de la série ISO/IEC 15408. Il comprend les éléments d'assurance individuels à partir desquels sont composés les niveaux d'assurance de l'évaluation et les autres paquets contenus dans l'ISO/IEC 15408-5, ainsi que les critères d'évaluation des profils de protection (PP), des configurations de PP, des modules de PP et des cibles de sécurité (ST).

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 15408-1:2026, *Sécurité de l'information — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 1: Introduction et modèle général*

ISO/IEC 15408-2:2026, *Sécurité de l'information — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 2: Composants fonctionnels 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 15408-5:2026, *Sécurité de l'information — Critères d'évaluation pour la sécurité des technologies de l'information — Partie 5: Paquets prédéfinis d'exigences 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*

ISO/IEC/IEEE 24765:2017, *Ingénierie des systèmes et du logiciel — Vocabulaire*

3 Termes et définitions

Pour les besoins du présent document, les termes et les définitions de l'ISO/IEC 15408-1, de l'ISO/IEC 15408-2, de l'ISO/IEC 18045 et de l'ISO/IEC IEEE 24765, 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
procédure d'acceptation
procédure suivie pour accepter un ou plusieurs *élément(s) de configuration* (3.4) nouvellement créé(s) ou modifié(s) comme faisant partie de la cible de l'évaluation (TOE), ou pour le déplacer vers l'étape suivante du cycle de vie

Note 1 à l'article: Ces procédures identifient les rôles ou individus responsables de l'acceptation ainsi que les critères à appliquer dans la décision d'acceptation.

Note 2 à l'article: Il existe plusieurs types de situations d'acceptation, dont certaines peuvent se chevaucher:

— l'acceptation d'un élément dans le système de gestion de configuration pour la première fois, en particulier dans le cadre d'un processus d'intégration;

— progression des éléments de configuration vers la phase suivante du cycle de vie à chaque étape de la construction de la TOE.

3.2
action
élément qui spécifie une activité entreprise par un évaluateur ou un développeur

Note 1 à l'article: Ces actions sont soit explicitement déclarées comme actions d'évaluateur, soit implicitement dérivées d'actions de développeur (actions d'évaluateur implicites) dans les composants d'assurance Voir 6.5 pour plus d'informations.

3.3
résultat réel des essais
résultat d'un essai qui peut être différent du résultat attendu des essais si le résultat réel des essais n'est pas égal au résultat attendu des essais

3.4
élément de configuration
élément ou agrégation de matériel, de logiciel ou des deux qui est conçu pour la gestion de configuration et traité comme une entité unique dans le processus de gestion de configuration pendant le *développement* (3.12) de la cible d'évaluation (TOE)

Note 1 à l'article: Il peut s'agir de parties de la TOE ou d'objets liés au développement de la TOE, par exemple des documents d'évaluation ou des outils de développement. Les éléments de gestion de configuration peuvent être stockés directement dans le système de gestion de configuration (p. ex. des fichiers) ou par voie de référence (p. ex. des pièces matérielles) avec leur version.

3.5
liste de configuration
document énumérant tous les *éléments de configuration* (3.4) pour un produit spécifique ainsi que la version exacte de chaque élément de gestion de configuration pertinent pour une version spécifique du produit complet

Note 1 à l'article: Cette liste permet de distinguer les éléments appartenant à la version évaluée du produit des autres versions de ces éléments appartenant à d'autres versions du produit. La liste de gestion de configuration finale est un document spécifique applicable à une version spécifique d'un produit spécifique. Cette liste peut, prendre la forme d'un document électronique à l'intérieur d'un *outil de gestion de configuration* (3.10). Dans ce cas, elle peut être considérée comme une vue spécifique sur le système ou une partie du système, plutôt que comme une donnée de sortie du système. Cependant, pour une utilisation pratique dans le cadre d'une évaluation, la liste de configuration sera probablement fournie dans le cadre de la documentation d'évaluation. La liste de configuration définit les éléments qui sont soumis aux exigences de gestion de la configuration des ALC_CMC (capacités CM) (12.2).

3.6
gestion de configuration
CM
discipline appliquant une orientation et une surveillance techniques et administratives pour identifier et documenter les caractéristiques fonctionnelles et physiques d'*éléments de configuration* (3.4), pour contrôler les changements apportés à ces caractéristiques, pour consigner et déclarer l'état de traitement et d'implémentation et pour vérifier la conformité aux exigences spécifiées

[SOURCE: ISO/IEC/IEEE 24765:2017, 3.779, modifié — La deuxième et troisième définitions ont été supprimées.]

3.7
documentation de la gestion de configuration
documentation de CM
documentation comprenant les *listes de configuration* (3.5) et les *plans de gestion de configuration* (3.8)

3.8
plan de gestion de configuration
plan de CM
description de la manière dont le *système de gestion de la configuration* (3.9) est utilisé pour la cible de l'évaluation (TOE)

Note 1 à l'article: L'objectif d'éditer un plan de gestion de configuration est de permettre aux membres du personnel de voir clairement ce qu'ils ont à faire. Du point de vue du système de gestion de configuration global, il peut être vu comme un document de sortie (car il peut être produit dans le cadre de l'application du système de gestion de configuration). Du point de vue du projet concret, il s'agit d'un document d'utilisation étant donné que les membres de l'équipe du projet l'utilisent pour comprendre les étapes qu'ils ont à effectuer tout au long du projet. Le plan de gestion de configuration définit l'usage du système pour le produit spécifique; le même système peut être utilisé dans une différente mesure pour d'autres produits. Le plan de gestion de configuration définit et décrit les données de sortie du système de gestion de configuration d'une entreprise qui sont utilisées au cours du *développement* (3.12). de la TOE.

Note 2 à l'article: La structure et le contenu d'un plan de gestion de configuration sont présentés dans l'ISO 10007:2017, Annexe A.

3.9
système de gestion de configuration
système CM
ensemble de procédures et d'outils (y compris leur documentation) utilisés par un développeur pour développer et maintenir les configurations de ses produits pendant leur cycle de vie

Note 1 à l'article: Les systèmes de gestion de configuration peuvent avoir des degrés de rigueur et de fonction variables. À des niveaux supérieurs, les systèmes de gestion de configuration peuvent être automatisés, avec une correction des défaillances, des contrôles des modifications et d'autres mécanismes de suivi.

3.10
outil de gestion de configuration
outil opéré manuellement ou automatisé, qui assure l'exécution ou la prise en charge d'un *système de gestion de configuration* (3.9)

EXEMPLE Outils de gestion de la version des parties de la cible d'évaluation (TOE).

3.11
livraison
transmission aux clients de la cible d'évaluation (TOE) finie depuis l'environnement de *production* (3.21)

Note 1 à l'article: Cette phase du cycle de vie du produit peut inclure l'emballage et le stockage sur le site de *développement* (3.12), mais ne comprend pas le transport de la TOE inachevée ou de parties de la TOE entre différents développeurs ou sites de développement différents.