Norme internationale

ISO/IEC 18045

Quatrième 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 — Exigences et méthodologie pour l'évaluation de sécurité

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

Numéro de référence
ISO/IEC 18045:2026(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 quatrième édition annule et remplace la troisième édition (ISO/IEC 18045:2022), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— le document a été aligné sur les modifications apportées à la série de normes ISO/IEC 15408;

— des changements techniques ont été introduits:

— la terminologie a été revue et mise à jour;

— les unités de travail de chaque composant ont été revues et mises à jour.

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 présent document est principalement destiné aux évaluateurs qui appliquent la série de normes ISO/IEC 15408 et aux certificateurs qui confirment les actions entreprises par les évaluateurs.

Peuvent constituer un public secondaire:

— les commanditaires de l'évaluation;

— les développeurs;

— les auteurs du profil de protection (PP), du module de PP, de la configuration de PP, et de la cible de sécurité (ST);

— les autres parties intéressées par la sécurité informatique.

Le présent document n'est pas destiné à répondre à toutes les questions relatives à l'évaluation de la sécurité informatique; des interprétations complémentaires peuvent être nécessaires. Des schémas individuels déterminent la manière de traiter ces interprétations, bien que celles-ci puissent faire l'objet d'accords de reconnaissance mutuelle. Une liste des activités relatives à la méthodologie qui peuvent être traitées par des schémas individuels figure à l'Annexe A.

Le présent document est destiné à être utilisé conjointement avec la série de normes ISO/IEC 15408.

Le présent document utilise des caractères italiques gras pour identifier des verbes particuliers relatifs aux activités d'évaluation obligatoires.

Plusieurs organisations gouvernementales ont contribué à l'élaboration de la présente version de la Méthodologie commune d'évaluation pour la sécurité des technologies de l'information. Par la présente, en tant que cotitulaires des droits d'auteur de la Méthodologie commune d'évaluation pour la sécurité des technologies de l'information (en abrégé, CEM), ces organisations accordent à l'ISO/IEC une licence non exclusive d'utilisation de la CEM pour poursuivre l'élaboration/la maintenance de la Norme internationale ISO/IEC 18045. Toutefois, lesdites organisations gouvernementales se réservent le droit d'utiliser, de copier, de diffuser, de traduire ou de modifier la CEM comme elles l'entendent. De plus amples informations concernant ces agences sont disponibles à l'adresse https://commoncriterialportal.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 — Exigences et méthodologie pour l'évaluation de sécurité

1 Domaine d'application

Le présent document spécifie les exigences et les actions minimales réalisées par un évaluateur pour mener une évaluation en utilisant les critères et les preuves d'évaluation définis dans l'évaluation de la série de normes ISO/IEC 15408.

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

ISO/IEC 15408-2:2026, *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 15408-4:2026, *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation de la sécurité informatique — Partie 4: Cadre prévu pour la spécification des méthodes d'évaluation et des activités connexes*

ISO/IEC 15408-5:2026, *Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation de la sécurité informatique — Partie 5: Paquets prédéfinis d'exigences de sécurité*

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 IEEE 24765, l'ISO/IEC 15408-1, l'ISO/IEC 15408-2, l'ISO/IEC 15408-3, 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
vérifier
⟨évaluation⟩ génération d'un verdict par une comparaison simple

Note 1 à l'article: L'expertise de l'évaluateur n'est pas requise. Les énoncés utilisant ce verbe «vérifier» décrivent les éléments mis en correspondance.

3.2
confirmer
⟨évaluation⟩ déclarer que quelque chose a été examiné en détail et que le caractère suffisant de cet examen a été déterminé de manière indépendante

Note 1 à l'article: Le niveau de rigueur dépend de la nature du sujet.

3.3
démontrer
⟨évaluation⟩ fournir une conclusion tirée d'une analyse moins rigoureuse que celle exigée par *prouver* (3.18)

3.4
décrire
⟨évaluation⟩ fournir certains détails spécifiques à une entité

3.5
déterminer
⟨évaluation⟩ affirmer un résultat particulier sur la base d'une analyse indépendante, dans l'objectif de parvenir à une conclusion donnée

Note 1 à l'article: L'emploi de ce terme implique une analyse véritablement indépendante, en général en l'absence de toute analyse antérieure. Cela est différent des termes *confirmer* (3.2) ou *contrôler* (3.29), qui impliquent qu'une analyse a déjà été effectuée et nécessite un examen.

3.6
temps écoulé
durée de temps totale nécessaire à un attaquant pour identifier l'existence d'une potentielle vulnérabilité particulière dans la cible d'évaluation (TOE), développer une méthode d'attaque et soutenir l'effort requis pour monter l'attaque contre la TOE

3.7
garantir
⟨évaluation⟩ montrer l'existence d'une forte relation de cause à effet entre une action et ses conséquences

Note 1 à l'article: Lorsque «garantir» est précédé du mot «aide à», cela indique que la conséquence n'est pas absolument certaine, sur la base de cette seule action.

3.8
autorité d'évaluation
entité qui établit et maintient un schéma, surveille l'évaluation menée par l'évaluateur et délivre des rapports de certification ou de validation ainsi que des certificats sur la base des résultats de l'évaluation fournis par l'évaluateur

3.9
preuve d'évaluation
élément utilisé comme base pour établir le verdict d'une activité d'évaluation

3.10
rapport technique d'évaluation
ETR
élément présentant une justification technique du ou des verdicts d'évaluation

3.11
examiner
⟨évaluation⟩ rendre un verdict au moyen d'une analyse faisant appel à l'expertise de l'évaluateur

Note 1 à l'article: Les énoncés utilisant ce verbe identifient les éléments analysés et les propriétés recherchées par l'analyse.

3.12
exhaustif/exhaustive
⟨évaluation⟩ caractéristique d'une approche méthodique adoptée pour effectuer une analyse ou une activité conformément à un plan univoque

Note 1 à l'article: Ce terme est utilisé dans les parties pertinentes de la série de normes ISO/IEC 15408 en ce qui concerne la conduite d'une analyse ou d'une autre activité. Il est lié au terme «systématique», mais dans un sens considérablement plus fort puisqu'il indique non seulement qu'une approche méthodique a été adoptée pour effectuer l'analyse ou l'activité conformément à un plan non ambigu, mais également que le plan suivi est suffisant pour *garantir* (3.7) que toutes les voies possibles ont été explorées.

3.13
expliquer
⟨évaluation⟩ donner un argument justifiant l'adoption d'un plan d'action

Note 1 à l'article: Ce terme a un sens différent des termes *décrire* (3.4) et *démontrer* (3.3). Il vise à répondre à la question «pourquoi?», sans essayer réellement de prétendre que la ligne de conduite qui a été choisie était nécessairement optimale.

3.14
justifier
⟨évaluation⟩ fournir un argumentaire apportant des motifs suffisants

Note 1 à l'article: Le terme «justifier» implique davantage de rigueur que le terme *démontrer* (3.3). Ce terme sous-entend une grande rigueur pour *expliquer* (3.13) très soigneusement et complètement chaque étape d'une analyse logique débouchant sur une conclusion.

3.15
attaque par surveillance
catégorie générique de méthodes d'attaque comprenant des techniques d'analyse passive visant à divulguer des données internes sensibles de la cible d'évaluation (TOE) en exploitant la TOE d'une manière compatible avec les guides d'utilisation fournis par le développeur

3.16
rapport d'observation
OR
rapport rédigé par l'évaluateur afin de demander une clarification ou identifiant un problème rencontré lors de l'évaluation

3.17
verdict de supervision
déclaration émise par une autorité d'évaluation afin de confirmer ou de rejeter le verdict global fondé sur les résultats des activités de supervision de l'évaluation

3.18
prouver
⟨évaluation⟩ montrer une correspondance à l'aide d'une analyse formelle au sens mathématique du terme

Note 1 à l'article: Cette action est totalement rigoureuse à tous points de vue. En règle générale, le terme «prouver» est utilisé lorsqu'il existe une volonté de montrer une correspondance entre deux représentations de fonctionnalité de sécurité (TSF) de la cible d'évaluation (TOE) à un niveau de rigueur élevé.

3.19
consigner
⟨évaluation⟩ conserver une description écrite des procédures, des événements, des observations, des indications et des résultats, suffisamment détaillée pour permettre de reconstituer ultérieurement le travail effectué au cours de l'évaluation

3.20
rapporter
⟨évaluation⟩ inclure les résultats d'évaluation et les supports dans le rapport technique d'évaluation, un *rapport d'observation* (3.16) ou un rapport de l'autorité d'évaluation

3.21
appliquant les SFR
fonctionnalité qui met en œuvre une exigence fonctionnelle de sécurité (SFR)

3.22
soutenant les SFR
fonctionnalité dont dépend une fonctionnalité *appliquant les exigences fonctionnelles de sécurité (SFR)* (3.21), mais qui n'a besoin de fonctionner correctement qu'afin que les politiques de sécurité de la cible d'évaluation (TOE) soient préservées

3.23
n'interférant pas avec les SFR
fonctionnalité envers laquelle ni une fonctionnalité *appliquant les exigences fonctionnelles de sécurité (SFR)* (3.21) ni une fonctionnalité *soutenant les SFR* (3.22) n'a de dépendance; c'est-à-dire, qu'elle ne joue aucun rôle dans la mise en œuvre de la fonctionnalité des SFR

3.24
spécifier
⟨évaluation⟩ fournir des détails spécifiques concernant une entité d'une manière rigoureuse et précise

3.25
sous-activité
application d'un composant d'assurance de l'ISO/IEC 15408-3:2026

Note 1 à l'article: Les familles d'assurance ne sont pas explicitement abordées dans la série de normes ISO/IEC 15408, car les évaluations sont menées sur un seul composant d'assurance d'une famille d'assurance.

3.26
tâche
travail d'évaluation spécifique à une méthodologie qui n'est pas déterminé directement à partir d'une exigence issue de la série de normes ISO/IEC 15408

3.27
tracer
⟨évaluation⟩ établir une relation entre deux ensembles d'entités, qui montre quelles entités du premier ensemble correspondent à quelles entités du second

3.28
verdict
déclaration de type émise par un évaluateur concernant une tâche de l'évaluateur, un composant ou une classe d'assurance

3.29
contrôler
⟨évaluation⟩ effectuer un examen détaillé rigoureux assorti de la détermination indépendante de son caractère suffisant

Note 1 à l'article: Voir également *confirmer* (3.2) qui a des connotations plus rigoureuses. Le terme «contrôler» est utilisé dans le contexte des actions d'un évaluateur qui nécessitent de sa part un effort indépendant.

3.30
fenêtre d'opportunité
période durant laquelle un attaquant a accès à la cible d'évaluation (TOE)

3.31
unité de travail
niveau le plus granulaire du travail d'évaluation

4 Terminologie

Contrairement à la série de normes ISO/IEC 15408, dans laquelle chaque élément conserve généralement le dernier chiffre de son symbole d'identification pour tous les composants de cette famille avec certaines exceptions, le présent document peut introduire de nouvelles unités de travail lorsqu'une action élémentaire d'un évaluateur de la série de normes ISO/IEC 15408 passe d'une sous-activité à une autre. De ce fait, le dernier chiffre du symbole d'identification de l'unité de travail peut changer même si l'unité de travail reste inchangée.

Tout travail d'évaluation spécifique à une méthodologie qui n'est pas déterminé directement à partir d'une exigence issue de la série de normes ISO/IEC 15408 est appelé tâche.

5 Utilisation des verbes

Tous les verbes d'unité de travail et de tâche sont précédés du verbe auxiliaire «doit»/«doivent». Les verbes d'unité de travail et de tâche ainsi que le verbe «doit» apparaissent en caractères ***italiques gras***. La forme verbale «***doit***» est utilisée uniquement lorsque le texte fourni est exigé et donc uniquement dans les unités de travail et les tâches. Les unités de travail et les tâches comprennent des activités exigées que l'évaluateur doit effectuer pour attribuer des verdicts.

Le texte de recommandation accompagnant les unités de travail et les tâches donne des explications supplémentaires sur la manière d'appliquer les termes de la série de normes ISO/IEC 15408 dans une évaluation.

6 Recommandations générales d'évaluation

Les matériaux qui s'appliquent à plus d'une sous-activité sont regroupés dans le présent document. Les recommandations dont l'applicabilité est étendue (au sein des activités et des EAL) ont été réunies dans l'Annexe A. Les recommandations concernant plusieurs sous-activités au sein d'une même activité ont été fournies dans l'introduction de cette activité. Si les recommandations ne concernent qu'une seule sous-activité, elles sont présentées au sein de celle-ci.

7 Relation entre les structures au sein de la CC et la structure du présent document

Il existe des relations directes entre les constructions d'assurance de la série de normes ISO/IEC 15408 et la structure du présent document. La Figure 1 illustre la correspondance entre les constructions de classes d'assurance, de composants d'assurance et d'éléments d'assurance de l'ISO/IEC 15408-3:2026 et les activités, sous-activités, actions et unités de travail de la méthodologie d'évaluation associée. Plusieurs unités de travail de la méthodologie d'évaluation peuvent résulter des exigences spécifiées dans les actions du développeur et les éléments de contenu et de présentation de la série de normes ISO/IEC 15408.