Norme internationale

ISO/IEC 18045

Troisième édition
2022-08

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Méthodologie pour l'évaluation de sécurité

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

Numéro de référence
ISO/IEC 18045:2022(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'attention est attirée sur le fait que certains des éléments du présent document peuvent faire l'objet de droits de propriété intellectuelle ou de droits analogues. L'ISO et l'IEC ne sauraient être tenues pour responsables de ne pas avoir identifié de tels droits de propriété et averti de leur existence. Les détails concernant les références aux droits de propriété intellectuelle ou autres droits analogues identifiés lors de l'élaboration du document sont indiqués dans l'Introduction et/ou dans la liste des déclarations de brevets reçues par l'ISO (voir www.iso.org/brevets) ou dans la liste des déclarations de brevets reçues par l'IEC (voir http://patents.iec.ch).

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/fr/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*.

Cette troisième édition annule et remplace la deuxième édition (ISO/IEC 18045:2008), qui a fait l'objet d'une révision technique.

Les principales modifications sont les suivantes:

— le type de conformité «exacte» a été introduit;

— les PP de faible assurance ont été supprimés et les PP à argumentaire direct ont été introduits;

— les modules de PP et les configurations de PP pour les évaluations modulaires ont été introduits;

— l'évaluation multi-assurance a été introduite.

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.

Mentions légales

Les organismes gouvernementaux énumérés ci-dessous ont contribué à l'élaboration de la présente version de la méthodologie commune pour l'évaluation de la sécurité des technologies de l'information. En tant que cotitulaires des droits d'auteur de la Méthodologie commune pour l'évaluation de la sécurité des technologies de l'information (appelée CEM), ils accordent par la présente une licence non exclusive à l'ISO/IEC pour l'utilisation de la CEM dans le cadre du développement et de la maintenance continus de la Norme internationale ISO/IEC 18045. Ces organismes gouvernementaux conservent toutefois le droit d'utiliser, de copier, de distribuer, de traduire ou de modifier la CEM comme ils l'entendent.»

Australie	The Australian Signals Directorate
Canada	Centre de la sécurité des télécommunications Canada (Communications Security Establishment)
France	Agence Nationale de la Sécurité des Systèmes d'Information
Allemagne	Bundesamt für Sicherheit in der Informationstechnik
Japon	Information-technology Promotion Agency
Pays-Bas	Netherlands National Communications Security Agency
Nouvelle-Zélande	Government Communications Security Bureau
République de Corée	Institut national de recherche en matière de sécurité
Espagne	Ministerio de Asuntos Económicos y Transformación Digital
Suède	FMV, Administration du matériel des armées
Royaume-Uni	National Cyber Security Centre
États-Unis	The National Security Agency

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. Les commanditaires de l'évaluation, les développeurs, les auteurs du profil de protection (PP), du module de PP et de la cible de sécurité (ST), ainsi que toute autre partie intéressée par la sécurité informatique, peuvent constituer un public secondaire.

Le présent document ne peut 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.

NOTE 1 Tout au long du document, les références à l'ISO/IEC 15408 se rapportent à la série de normes ISO/IEC 15408.

NOTE 2 Dans certains cas, le présent document utilise des caractères gras et italiques pour distinguer des termes du reste du texte. Les relations entre les composants d'une famille sont mises en évidence par l'utilisation de caractères gras. Cette convention d'écriture impose les caractères gras à toute nouvelle exigence. Pour les composants en relation hiérarchique, les exigences sont écrites en caractères gras lorsqu'elles sont étendues ou modifiées au-delà des exigences relatives au composant précédent. En outre, toute opération nouvelle ou étendue permise et allant au-delà du composant précédent est également mise en évidence en utilisant des caractères gras.

L'utilisation de caractères en italique indique que le terme correspondant revêt un sens précis. Concernant les exigences d'assurance de sécurité, la convention concerne des verbes spécifiques ayant trait à l'évaluation.

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Méthodologie pour l'évaluation de sécurité

1 Domaine d'application

Le présent document définit les actions minimales à réaliser par un évaluateur pour mener une évaluation selon la série de normes ISO/IEC 15408 en utilisant les critères et les preuves d'évaluation définis dans 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 15408-1:2022, *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 15408-2:2022, *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 15408-3:2022, *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 de spécification de méthodes et activités d'évaluation*

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 en matière de sécurité*

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

3 Termes et définitions

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, l'ISO/IEC 15408-4, l'ISO/IEC 15408-5, l'ISO/IEC IEEE 24765, ainsi que les suivants s'appliquent.

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. L'énoncé qui utilise ce verbe décrit ce qui est 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 qu'une «preuve»

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. À distinguer des termes *«confirmer»* (3.2) ou *«contrôler»* (3.22), qui impliquent qu'une analyse a déjà été effectuée et qu'elle nécessite une vérification.

3.6
potentielle vulnérabilité rencontrée
faiblesse potentielle dans la cible d'évaluation (TOE), identifiée par l'évaluateur lors d'activités d'évaluation et qui peut être exploitée pour violer les exigences fonctionnelles de sécurité (SFR)

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

3.9
examiner
<évaluation> rendre un verdict au moyen d'une analyse faisant appel à l'expertise de l'évaluateur

Note 1 à l'article: L'énoncé qui utilise ce verbe identifie les éléments analysés et les propriétés recherchées par l'analyse.

3.10
exhaustif
<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.

3.11
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.

3.12
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* (3.11) très soigneusement et complètement chaque étape d'une analyse logique débouchant sur une conclusion .

3.13
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

3.14
rapport d'observation
OR
rapport rédigé par l'évaluateur afin de demander une clarification ou identifiant un problème rencontré lors de l'évaluation

3.15
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

3.16
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.

3.17
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

3.18
rapporter
<évaluation> inclure les résultats d'évaluation et les supports dans le rapport technique d'évaluation, un *rapport d'observation* (3.14) ou un rapport de l'autorité d'évaluation

3.19
spécifier
<évaluation> fournir des détails spécifiques concernant une entité d'une manière rigoureuse et précise

3.20
tracer
<évaluation> établir une relation entre deux ensembles d'entités, qui montre quelles entités du premier ensemble correspondent à quelles entités du second

3.21
verdict
déclaration de type émise par un évaluateur concernant une tâche de l'évaluateur, un composant ou une classe d'assurance

3.22
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). Ce terme possède 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.

3.23
fenêtre d'opportunité
période durant laquelle un attaquant a accès à la cible d'évaluation (TOE)

3.24
unité de travail
niveau le plus fin du travail d'évaluation

4 Abréviations

OR rapport d'observation (Observation Report)

5 Terminologie

Contrairement à la série de normes ISO/IEC 15408, dans laquelle chaque élément conserve le dernier chiffre de son symbole d'identification pour tous les composants de cette famille, 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* ou *sous-tâche*.

6 Utilisation des verbes

Tous les verbes relatifs aux unités de travail et aux sous-tâches sont précédés de la forme verbale «*doit*» et par la présentation du verbe et de la forme verbale «*doit*» en caractères ***italiques gras***. La forme verbale «*doit*» est utilisée uniquement lorsque le texte fourni est obligatoire et donc uniquement dans les unités de travail et les sous-tâches. Les unités de travail et les sous-tâches comprennent des activités obligatoires que l'évaluateur doit effectuer pour attribuer des verdicts.

Le texte de recommandation accompagnant les unités de travail et les sous-tâches donne des explications supplémentaires sur la manière d'appliquer les termes de l'ISO/IEC 15408 dans une évaluation. L'utilisation des verbes est conforme aux définitions de l'ISO pour ces verbes. La formule «il convient que» est utilisée pour indiquer une recommandation. «Peut» («*may*» en anglais) indique parfois une autorisation, ou encore («*can*» en anglais) une possibilité ou une capacité.

Les verbes *vérifier*, *examiner*, *rapporter* et *consigner* sont utilisés avec une signification précise dans cette partie du présent document et il convient de faire référence à l'Article 3 pour leurs définitions.

7 Recommandations générales d'évaluation

Les matériaux qui s'appliquent à plus d'une sous-activité sont rassemblés en un seul endroit. Les recommandations dont l'applicabilité est étendue (au sein des activités et des EAL) ont été réunies dans