NORME INTERNATIONALE

ISO/IEC 18045

Deuxième édition
2008-08-15

Technologies de l'information — Techniques de sécurité — Méthodologie pour l'évaluation de sécurité TI

Information technology — Security techniques — Methodology for IT security evaluation

Numéro de référence
ISO/IEC 18045:2008(F)

ISO copyright office
Case postale 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Genève
Tél.: +41 22 749 01 11
Fax: +41 22 749 09 47
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. Dans le domaine des technologies de l'information, l'ISO et l'IEC ont créé un comité technique mixte, l'ISO/IEC JTC 1.

Les Normes internationales sont rédigées conformément aux règles données dans les Directives ISO/IEC, Partie 2.

La tâche principale du comité technique mixte est d'élaborer les Normes internationales. Les projets de Normes internationales adoptés par le comité technique mixte sont soumis aux organismes nationaux pour vote. Leur publication comme Normes internationales requiert l'approbation de 75 % au moins des organismes nationaux votants.

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.

L'ISO/IEC 18045 a été élaborée par le comité technique mixte ISO/IEC JTC 1, *Technologies de l'information*, sous-comité SC 27, *Techniques de sécurité des technologies de l'information*. Le texte identique de l'ISO/IEC 18045 est publié par les organisations commanditaires du projet Critères communs sous le titre *Common Methodology for Information Technology Security Evaluation* (Méthodologie commune pour l'évaluation de la sécurité des technologies de l'information). La source XML commune aux deux publications peut être obtenue à l'adresse http://www.commoncriteriaportal.org/cc/.

Cette deuxième édition annule et remplace la première édition (ISO/IEC 18045:2005), qui a fait l'objet d'une révision technique.

La présente version française de l'ISO ISO/IEC 18045:2008 correspond à la version anglaise publiée le 2008-08 et corrigée le 2014-01.

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, version 3.1 (appelée CEM 3.1), ils accordent par la présente une licence non exclusive à l'ISO/IEC pour l'utilisation de la CEM 3.1 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 3.1 comme ils l'entendent.

Australie/Nouvelle-Zélande:	Defence Signals Directorate et Government Communications Security Bureau, respectivement;
Canada:	Centre de la sécurité des télécommunications Canada (Communications Security Establishment);
France:	Direction Centrale 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;
Espagne:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
Royaume-Uni:	Communications-Electronic Security Group;
États-Unis:	National Security Agency et National Institute of Standards and Technology.

Introduction

La présente Norme internationale est principalement destinée aux évaluateurs appliquant l'ISO/IEC 15408 et aux certificateurs confirmant les actions des évaluateurs; les commanditaires de l'évaluation, les développeurs, les auteurs de PP/ST et les autres parties intéressées par la sécurité informatique peuvent constituer un public secondaire.

La présente Norme internationale reconnaît qu'elle ne répond pas à toutes les questions concernant l'évaluation de la sécurité informatique et que des interprétations supplémentaires seront nécessaires. Des schémas individuels détermineront 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.

Technologies de l'information — Techniques de sécurité — Méthodologie pour l'évaluation de sécurité TI

1 Domaine d'application

La présente Norme internationale est un document complémentaire de l'ISO/IEC 15408 «Critères d'évaluation pour la sécurité TI». La présente Norme internationale définit les actions minimales à réaliser par un évaluateur pour mener une évaluation selon l'ISO/IEC 15408 en utilisant les critères et les preuves d'évaluation définies dans l'ISO/IEC 15408.

La présente Norme internationale ne définit pas les actions de l'évaluateur pour certaines exigences d'assurance de haut niveau de l'ISO/IEC 15408 lorsqu'il n'existe pas encore de recommandations généralement reconnues.

2 Références normatives

Les documents de référence suivants sont indispensables pour l'application 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 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent.

NOTE Les termes présentés en caractères gras sont eux-mêmes définis dans le présent paragraphe.

3.1
action
élément d'action de l'évaluateur de l'ISO/IEC 15408-3

Note 1 à l'article: Ces actions sont soit explicitement mentionnées comme des actions de l'évaluateur, soit implicitement dérivées d'actions du développeur (actions implicites de l'évaluateur) dans le cadre des composants d'assurance de l'ISO/IEC 15408-3.

3.2
activité
application d'une classe d'assurance de l'ISO/IEC 15408-3

3.3
vérifier
génération d'un **verdict** par une simple comparaison

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.

3.4
livrable d'évaluation
toute ressource requise du commanditaire ou du développeur par l'évaluateur ou l'autorité d'évaluation afin de réaliser une ou plusieurs activités d'évaluation ou de supervision de l'évaluation

3.5
preuve d'évaluation
livrable d'évaluation matériel

3.6
rapport technique d'évaluation
rapport qui documente le **verdict global** et sa justification, généré par l'évaluateur et soumis à une autorité d'évaluation

3.7
examiner
générer 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 pour lesquelles ceux-ci sont analysés.

3.8
interprétation
clarification ou amplification d'une exigence de l'ISO/IEC 15408, de l'ISO/IEC 18045 ou d'une exigence relative à un **schéma**

3.9
méthodologie
système de principes, de procédures et de processus appliqué aux évaluations de sécurité TI

3.10
rapport d'observation
rapport rédigé par l'évaluateur afin de demander une clarification ou l'identification d'un problème rencontré lors de l'évaluation

3.11
verdict global
déclaration de type *réussite ou échec* émise par un évaluateur concernant le résultat d'une évaluation

3.12
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

3.13
consigner
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

3.14
rapporter
inclure les résultats de l'évaluation et les éléments justificatifs dans le **rapport technique d'évaluation** ou dans un **rapport d'observation**

3.15
schéma
ensemble de règles, établies par une autorité d'évaluation, définissant l'environnement d'évaluation, y compris les critères et la **méthodologie** nécessaires pour mener des évaluations de la sécurité des TI

3.16
sous-activité
application d'un composant d'assurance de l'ISO/IEC 15408-3

Note 1 à l'article: Les familles d'assurance ne sont pas explicitement abordées dans la présente Norme internationale car les évaluations sont menées sur un seul composant d'assurance d'une famille d'assurance.

3.17
traçabilité
simple relation directionnelle entre deux ensembles d'entités, qui montre quelles entités du premier ensemble correspondent à quelles entités du second

3.18
verdict
déclaration de type *réussite, échec ou non concluant* émise par un évaluateur concernant un élément d'action d'évaluateur, un composant d'assurance ou une classe d'évaluation selon l'ISO/IEC 15408

Note 1 à l'article: Voir également **verdict global**.

3.19
unité de travail
niveau le plus granulaire du travail d'évaluation

Note 1 à l'article: Chaque action de méthodologie d'évaluation comprend une ou plusieurs unités de travail, qui sont regroupées au sein de l'action de méthodologie d'évaluation par le contenu et la présentation des preuves de l'ISO/IEC 15408 ou l'élément d'action du développeur. Les unités de travail sont présentées dans la présente Norme internationale dans le même ordre que les éléments de l'ISO/IEC 15408 dont elles sont dérivées. Les unités de travail sont identifiées dans la marge gauche par un symbole tel que ALC_TAT.1-2. Dans ce symbole, la chaîne *ALC_TAT.1* indique l'élément de l'ISO/IEC 15408 (c'est-à-dire cette sous-activité de la Norme internationale), et le dernier chiffre (2) indique qu'il s'agit de la deuxième unité de travail de la sous-activité ALC_TAT.1.

4 Symboles et abréviations

RO Rapport d'observation (Observation Report)

RTE Rapport technique d'évaluation (Évaluation Technical Report)

5 Présentation générale

5.1 Organisation de la présente Norme internationale

L'Article 6 définit les conventions utilisées dans la présente Norme internationale.

L'Article 7 décrit les tâches d'évaluation générales sans verdict associé car elles ne correspondent pas aux éléments d'action de l'évaluateur de l'ISO/IEC 15408.

L'Article 8 aborde la quantité de travail nécessaire pour obtenir un résultat d'évaluation sur un PP.

Les Articles 9 à 15 définissent les activités d'évaluation, organisées par classes d'assurance.

L'Annexe A couvre les techniques d'évaluation de base utilisées pour fournir des preuves techniques de résultats d'évaluation.

L'Annexe B fournit une explication des critères d'analyse de la vulnérabilité et des exemples de leur application.

6 Conventions relatives aux documents

6.1 Terminologie

Contrairement à l'ISO/IEC 15408, où chaque élément conserve le dernier chiffre de son symbole d'identification pour tous les composants de la famille, la présente Norme internationale peut introduire de nouvelles unités de travail lorsqu'un élément d'action d'évaluateur de l'ISO/IEC 15408 change d'une sous-activité à l'autre; par conséquent, le dernier chiffre du symbole d'identification de l'unité de travail peut changer bien que l'unité de travail reste la même.

Tout travail d'évaluation spécifique à une méthodologie qui n'est pas déterminé directement à partir des exigences de l'ISO/IEC 15408 est appelé *tâche* ou *sous-tâche*.

6.2 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 contiennent 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 forme verbale «*il convient que*» est utilisée lorsque la méthode décrite est fortement préférée. Tous les autres formes verbales, y compris «*peut*», sont utilisées lorsque la ou les méthodes décrites sont autorisées, mais ne sont ni recommandées ni fortement préférées; il s'agit simplement d'une explication.

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

6.3 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 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.

6.4 Relation entre les structures de l'ISO/IEC 15408 et de l'ISO/IEC 18045

Il existe des relations directes entre la structure de l'ISO/IEC 15408 (c'est-à-dire, classe, famille, composant et élément) et la structure de la présente Norme internationale. La Figure 1 illustre la correspondance entre les constructions des classes, des familles et des éléments d'action d'évaluateur et des activités, sous-activités et actions de la méthodologie d'évaluation de l'ISO/IEC 15408. Toutefois, plusieurs unités de travail de la méthodologie d'évaluation peuvent résulter des exigences notées dans les actions du développeur et les éléments de contenu et de présentation de l'ISO/IEC 15408.

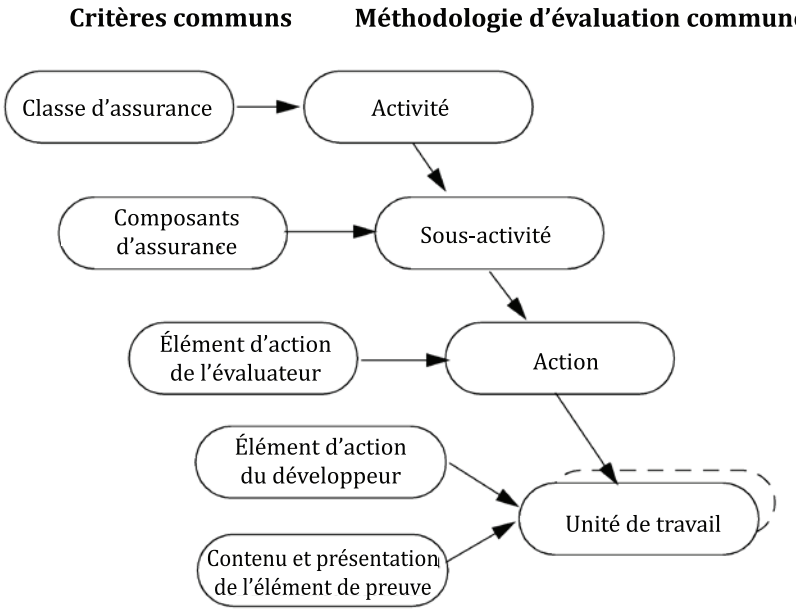

Figure 1 — Mise en correspondance des structures de l'ISO/IEC 15408 et de l'ISO/IEC 18045

7 Processus d'évaluation et tâches associées

7.1 Introduction

Le présent article donne un aperçu du processus d'évaluation et définit les tâches qu'un évaluateur est censé accomplir lorsqu'il procède à une évaluation.

Chaque évaluation, qu'il s'agisse d'un profil de protection (PP, Protection Profile) ou d'une cible d'évaluation (TOE, Target of Evaluation), cible de sécurité (ST, Security Target) comprise, suit le même processus et possède quatre tâches d'évaluateur en commun: la tâche d'entrée, la tâche de sortie, les sous-activités d'évaluation et la démonstration de la compétence technique pour la tâche de l'autorité d'évaluation.

La tâche d'entrée et les tâches de sortie, qui sont liées à la gestion des preuves d'évaluation et à la production de rapports, sont entièrement décrites dans le présent article. Chaque tâche est associée à des sous-tâches qui s'appliquent et sont normatives pour toutes les évaluations selon l'ISO/IEC 15408 (évaluation d'un PP ou d'une TOE).

Les sous-activités d'évaluation sont uniquement introduites dans le présent article, et sont entièrement décrites dans les articles suivants.

Contrairement aux sous-activités d'évaluation, les tâches d'entrée et de sortie ne sont pas associées à des verdicts car elles ne correspondent pas aux éléments d'action de l'évaluateur de l'ISO/IEC 15408; elles sont réalisées afin de garantir la conformité avec les principes universels et la conformité à la présente Norme internationale.

La démonstration de la compétence technique pour la tâche de l'autorité d'évaluation peut être réalisée par l'analyse des résultats des tâches de sortie par l'autorité d'évaluation, ou peut inclure la démonstration par les évaluateurs de leur compréhension des données d'entrées concernant les sous-activités d'évaluation. Cette tâche n'est pas associée à un verdict de l'évaluateur, mais à un verdict de l'autorité d'évaluation. Les critères détaillés concernant la réalisation de cette tâche sont laissés à la discrétion de l'autorité d'évaluation, comme indiqué à l'Annexe 0.