NORME INTERNATIONALE

ISO/IEC 19896-3

Première édition
2018-08

Techniques de sécurité IT — Exigences de compétence pour les testeurs et les évaluateurs en matière de sécurité de l'information —

Partie 3: Exigences en matière de connaissances, compétences et efficacité des spécialistes en évaluations ISO/IEC 15408

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/iso/

IT security techniques — Competence requirements for information security testers and evaluators —

Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

Numéro de référence
ISO/IEC 19896-3:2018(F)

© ISO/IEC 2018

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/d8afeb32-2f33-4ccd-8e89-d462b67840e1/iso-iec-19896-3-2018

DOCUMENT PROTÉGÉ PAR COPYRIGHT

© ISO/IEC 2018

Tous droits réservés. Sauf prescription différente ou nécessité dans le contexte de sa mise en œuvre, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie, ou la diffusion sur l'internet ou sur un intranet, sans autorisation écrite préalable. Une autorisation peut être demandée à l'ISO à l'adresse ci-après ou au comité membre de l'ISO dans le pays du demandeur.

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 ..... **v**
Introduction ..... **vi**
1 Domaine d'application **1**
2 Références normatives **1**
3 Termes et définitions **1**
4 Connaissances **2**
4.1 Généralités 2
4.2 Connaissance de l'ISO/IEC 15408 et de l'ISO/IEC 18045 2
4.2.1 ISO/IEC 15408-1 2
4.2.2 ISO/IEC 15408-2 2
4.2.3 ISO/IEC 15408-3 3
4.2.4 ISO/IEC 18045 3
4.3 Connaissance du paradigme de l'assurance 3
4.3.1 Connaissance de l'autorité d'évaluation 3
4.3.2 Connaissance du schéma d'évaluation 4
4.3.3 Connaissance du laboratoire et de son système de management 4
4.4 Connaissance de la sécurité de l'information 4
4.5 Connaissance de la technologie évaluée 5
4.5.1 Connaissance de la technologie évaluée 5
4.5.2 Profils de protection, paquets et documents connexes 5
4.6 Connaissances requises pour des classes d'assurance spécifiques 6
4.7 Connaissances requises lors de l'évaluation d'exigences fonctionnelles de sécurité spécifiques 6
4.8 Connaissances nécessaires lors de l'évaluation de technologies spécifiques 6
5 Savoir-faire **6**
5.1 Savoir-faire d'évaluation de base 6
5.1.1 Méthodes d'évaluation 6
5.1.2 Outils d'évaluation 6
5.2 Savoir-faire d'évaluation de base spécifiés dans l'ISO/IEC 15408-3 et l'ISO/IEC 18045 7
5.2.1 Principes de l'évaluation 7
5.2.2 Méthodes et activités d'évaluation 7
5.3 Savoir-faire requis lors de l'évaluation de classes d'assurance de sécurité spécifiques 8
5.3.1 Généralités 8
5.3.2 Classe ADV (Développement) 8
5.3.3 Classe AGD (Manuels utilisateur) 9
5.3.4 Classe ALC (Prise en charge du cycle de vie) 9
5.3.5 Classes ASE et APE (évaluation ST et PP) 10
5.3.6 Classe ATE (Essais) 11
5.3.7 Classe AVA (Évaluation de la vulnérabilité) 11
5.3.8 Classe ACO (Composition) 12
5.4 Savoir-faire requis lors de l'évaluation de classes d'exigences fonctionnelles de sécurité spécifiques 13
5.4.1 Généralités 13
5.4.2 Savoir-faire requis lors de l'évaluation de la classe FCS (Support cryptographique) 13
5.5 Savoir-faire nécessaires lors de l'évaluation de technologies spécifiques 13
6 Expérience **13**
7 Instruction **13**
8 Efficacité **14**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/d8afeb32-2f33-4ccd-8e89-d462b67840e1/iso-iec-19896-3-2018

8.1 Généralités ... 14
8.2 Efficacité de l'évaluation ... 14
8.3 Responsabilités des schémas d'évaluation concernant l'efficacité des évaluateurs ... 14
8.4 Efficacité pour la réalisation d'évaluations en temps opportun ... 14
8.5 Efficacité pour la réalisation d'évaluations exactes ... 14
8.6 Efficacité concernant le rapportage des résultats ... 15

Annexe A (informative) **Types de technologie: Connaissances et savoir-faire** ... **16**

Annexe B (informative) **Exemples de connaissances requises pour l'évaluation des classes d'exigences d'assurance de la sécurité** ... **21**

Annexe C (informative) **Exemples de connaissances requises pour l'évaluation des classes d'exigences fonctionnelles de sécurité** ... **29**

Bibliographie ... **33**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/d8afeb32-2f33-4ccd-8e89-d462b67840e1/iso-iec-19896-3-2018

© ISO/IEC 2018 – Tous droits réservés

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 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 ISO. Le présent document a été rédigé conformément aux règles de rédaction données dans les Directives ISO/IEC, Partie 2 (voir www.iso.org/directives).

L'attention est appelée 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).

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.html.

Le présent document a été élaboré par le comité technique ISO/IEC JTC 1, Technologies de l'information, sous-comité SC 27, *Sécurité de l'information, cybersécurité et protection de la vie privée*.

Une liste de toutes les parties de la série ISO/IEC 19896 se trouve sur le site web de l'ISO.

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/fr/members.html.

© ISO/IEC 2018 – Tous droits réservés

Introduction

La série ISO/IEC 15408 permet la comparaison entre des résultats d'évaluations de sécurité indépendantes. À cet effet, elle propose un ensemble commun d'exigences applicables aux fonctionnalités de sécurité des produits de technologies de l'information (IT) et aux mesures d'assurance appliquées à ces produits IT au cours d'une évaluation de sécurité. De nombreux schémas de certification et d'évaluation ainsi que des autorités d'évaluation ont été élaborés en utilisant la série ISO/IEC 15408 et l'ISO/IEC 18045 comme base, ce qui permet de comparer les résultats des projets d'évaluation.

Un facteur important pour assurer la comparaison des résultats de ces évaluations consiste à comprendre que le processus d'évaluation inclut la spécification de mesures d'assurance à la fois objectives et subjectives. Par conséquent, la compétence des évaluateurs individuels est importante lorsque la comparaison et la répétabilité des résultats de l'évaluation constituent le fondement de la reconnaissance mutuelle.

L'ISO/IEC 17025 fournit des exigences générales concernant la compétence des laboratoires d'essai et d'étalonnage. Dans l'ISO/IEC 17025:2017, 5.2.1, il est précisé que *« le personnel effectuant des tâches spécifiques doit être qualifié sur la base d'une instruction, d'une formation, d'une expérience appropriées et/ou d'un savoir-faire démontré »*.

Le présent document établit une base de référence pour les compétences minimales des évaluateurs de l'ISO/IEC 15408 dans le but d'établir la conformité des exigences de formation des évaluateurs professionnels selon l'ISO/IEC 15408 associés aux programmes d'évaluation et aux autorités des produits IT. Il fournit les exigences spécifiques permettant de démontrer la compétence des personnes pour effectuer des évaluations de la sécurité des produits IT conformément à l'ISO/IEC 15408 (toutes les parties) et à l'ISO/IEC 18045. L'ISO/IEC 15408-1 décrit le cadre général des compétences, y compris les différents éléments de la compétence: connaissances, savoir-faire, expérience, instruction et efficacité. Le présent document inclut notamment les connaissances et les savoir-faire dans les domaines suivants.

iTeh Standards (https://standards.iteh.ai) Document Preview ISO/IEC 19896-3:2018 https://standards.iteh.ai/catalog/standards/sist/d8efeb32-2f2a-4ccd-8e89-d46f2b678d0e/iso-iec-19896-3-2018

— Sécurité de l'information

  Connaissances: Principes de sécurité de l'information, propriétés de sécurité de l'information, menace et vulnérabilités en matière de sécurité de l'information

  Savoir-faire: Comprendre les exigences en matière de sécurité de l'information, comprendre le contexte

— Évaluation de la sécurité de l'information

  Connaissances: Connaissance de l'ISO/IEC 15408 (toutes les parties) et de l'ISO/IEC 18045, système de management de laboratoire

  Savoir-faire: Savoir-faire de base en matière d'évaluation, savoir-faire essentiels en matière d'évaluation, savoir-faire requis lors de l'évaluation de classes d'assurance de la sécurité spécifiques, savoir-faire requis lors de l'évaluation de classes d'exigences fonctionnelles de sécurité spécifiques

— Architecture des systèmes d'information

  Connaissances: Technologie évaluée

  Savoir-faire: Comprendre l'interaction entre les composants de sécurité et les informations

— Essais de sécurité de l'information

  Connaissances: Techniques d'essai de la sécurité de l'information, outils d'essai de la sécurité de l'information, cycle de vie du développement des produits, types d'essais

  Savoir-faire: Créer et gérer un plan d'essai de sécurité de l'information, concevoir des essais de sécurité de l'information, préparer et réaliser des essais de sécurité de l'information

© ISO/IEC 2018 – Tous droits réservés

Le public visé par le présent document comprend les autorités de validation et de certification, les organismes de certification des laboratoires d'essai, les schémas d'évaluation, les laboratoires, les évaluateurs et les organismes proposant des certifications professionnelles.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/d8afeb32-2f33-4ccd-8e89-d462b67840e1/iso-iec-19896-3-2018

© ISO/IEC 2018 – Tous droits réservés

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/d8afeb32-2f33-4ccd-8e89-d462b67840e1/iso-iec-19896-3-2018

Techniques de sécurité IT — Exigences de compétence pour les testeurs et les évaluateurs en matière de sécurité de l'information —

Partie 3:
Exigences en matière de connaissances, compétences et efficacité des spécialistes en évaluations ISO/IEC 15408

1 Domaine d'application

Le présent document fournit les exigences spécifiques permettant de démontrer la compétence des personnes pour effectuer des évaluations de la sécurité des produits IT conformément à l'ISO/IEC 15408 (toutes les parties) et à l'ISO/IEC 18045.

2 Références normatives

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/d8afeb32-2f33-4ccd-8e89-d462b67840e1/iso-iec-19896-3-2018

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 19896-1, *Techniques de sécurité IT — Exigences de compétence pour les testeurs et les évaluateurs en matière de sécurité de l'information — Partie 1: Introduction, concepts et exigences générales*

ISO/IEC 15408 (toutes les parties), *Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI*

ISO/IEC 18045, *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*

ISO/IEC 17025, *Exigences générales concernant la compétence des laboratoires d'étalonnages et d'essais*

3 Termes et définitions

Pour les besoins du présent document, les termes et définitions donnés dans l'ISO/IEC 19896-1, l'ISO/IEC 15408-1 et l'ISO/IEC 17025, l'ISO/IEC 18045 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
schéma d'évaluation
organisation qui assure la mise en œuvre des politiques et d'un 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 IT

© ISO/IEC 2018 – Tous droits réservés

3.2
méthode subjective
méthode fondée sur l'expérience et la compréhension d'une personne donnée

4 Connaissances

4.1 Généralités

Les connaissances sont ce qu'un évaluateur connaît et peut décrire. Les paragraphes 4.2 à 4.8 traitent des connaissances nécessaires pour l'évaluation selon l'ISO/IEC 15408 (toutes les parties) et l'ISO/IEC 18045.

4.2 Connaissance de l'ISO/IEC 15408 et de l'ISO/IEC 18045

4.2.1 ISO/IEC 15408-1

Tous les évaluateurs doivent avoir connaissance des éléments suivants:

a) les termes et définitions définis dans l'ISO/IEC 15408-1;

b) les termes et définitions définis dans l'ISO/IEC 18045;

c) le contexte pour les évaluations selon l'ISO/IEC 15408;

d) le modèle général de la série ISO/IEC 15408 donné dans l'ISO/IEC 15408-1;

e) la personnalisation des exigences de sécurité: opérations, dépendances entre composants et composants étendus;

f) les profils et les paquets de protection;

g) les résultats de l'évaluation; et

h) la spécification des cibles de sécurité.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/d8afeb32-2f33-4ccd-8e89-d462b67840e1/iso-iec-19896-3-2018

4.2.2 ISO/IEC 15408-2

Tous les évaluateurs doivent avoir connaissance des exigences fonctionnelles de sécurité (SFR) de l'ISO/IEC 15408-2 qui sont utilisées pour les types de technologie avec lesquels l'évaluateur est autorisé à travailler, ainsi que de toute SFR dépendante. Les classes de SFR données dans l'ISO/IEC 15408-2 sont les suivantes:

a) audit de sécurité (FAU);

b) communication (FCO);

c) support cryptographique (FCS);

d) protection des données utilisateur (FDP);

e) identification et authentification (FIA);

f) gestion de la sécurité (FMT);

g) confidentialité des données (FPR);

h) protection des fonctions de sécurité de la cible d'évaluation (FPT);

i) utilisation des ressources (FRU);

j) accès à la cible d'évaluation (FTA); et

© ISO/IEC 2018 – Tous droits réservés

k) chemin/canaux de confiance (FTP).

4.2.3 ISO/IEC 15408-3

Tous les évaluateurs doivent avoir connaissance des exigences d'assurance de sécurité (SAR) données dans l'ISO/IEC 15408-3 qui sont spécifiées par les cibles de sécurité (ST) avec lesquelles l'évaluateur est autorisé à travailler. La connaissance des composants particuliers de SAR doit comprendre ceux pour lesquels l'évaluateur est autorisé à travailler. Les classes de SAR données dans l'ISO/IEC 15408-3 sont les suivantes:

a) développement (ADV);

b) manuel utilisateur (AGD);

c) prise en charge du cycle de vie (ALC);

d) structure de la cible de sécurité (ASE);

e) structure du profil de protection (APE);

f) essais (ATE);

g) évaluation de la vulnérabilité (AVA); et

h) composition (ACO).

iTeh STANDARD PREVIEW
(standards.iteh.ai)

4.2.4 ISO/IEC 18045

Tous les évaluateurs doivent avoir connaissance des éléments suivants:

a) le processus d'évaluation: ce processus est décrit dans l'ISO/IEC 18045:2008, Article 8; et

b) la méthode et les activités d'évaluation de la sécurité: ces informations sont données dans l'ISO/IEC 18045.

ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/d8a1eb32-2133-4ccd-8e89-d462b67840e1/iso-iec-19896-3-2018

4.3 Connaissance du paradigme de l'assurance

4.3.1 Connaissance de l'autorité d'évaluation

Tous les évaluateurs doivent avoir connaissance des exigences de l'autorité ou des autorités d'évaluation applicables aux schémas d'évaluation pour lesquels ils sont autorisés à travailler.

NOTE Parmi ces autorités d'évaluation, on peut par exemple citer l'« Accord de reconnaissance des critères communs (CCRA, *Common Criteria Recognition Agreement*) » et le « Groupe des hauts fonctionnaires pour la sécurité des systèmes d'information (SOG-IS, *Senior Officials Group Information Systems Security*) ».

Les exigences des autorités d'évaluation peuvent porter sur des sujets tels que:

a) le domaine d'application de l'autorité d'évaluation;

b) les accords de reconnaissance;

c) les politiques de l'autorité d'évaluation;

d) les recommandations pour les schémas d'évaluation, les valideurs et les évaluateurs;

e) les interprétations;

f) les documents d'appui;

g) la connaissance des normes connexes; et

© ISO/IEC 2018 – Tous droits réservés

h) les exigences en matière de qualité.

4.3.2 Connaissance du schéma d'évaluation

Les schémas d'évaluation définissent généralement des aspects opérationnels tels que les politiques et les modes opératoires qui sont spécifiques au schéma d'évaluation. Ces éléments sont souvent basés sur le domaine d'application du schéma d'évaluation.

Tous les évaluateurs doivent avoir connaissance des éléments suivants:

a) les exigences du ou des schémas d'évaluation pour lesquels ils sont autorisés à travailler;

EXEMPLES

— toute politique, réglementation et législation spécifiques au secteur;

— les exigences d'approbation des laboratoires pour le système d'évaluation;

— les politiques du schéma d'évaluation en ce qui concerne les projets d'évaluation, y compris les critères d'entrée, les limites de durée, les exigences en matière de rapports, les exigences en matière de visites sur site;

— les recommandations pour les valideurs et les évaluateurs;

— les interprétations spécifiques du schéma d'évaluation;

— les recommandations spécifiques du schéma d'évaluation;

— les profils de protection approuvés et leurs documents connexes;

— les méthodes et activités d'assurance spécifiques du schéma d'évaluation; et

— les exigences d'établissement de rapports.

b) les exigences de compétences du schéma d'évaluation concernant les évaluateurs.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/d8afe052-2155-4ced-8c89-d462b67840e1/iso-iec-19896-3-2018

NOTE À ce sujet, voir l'ISO/IEC 18045:2008, A.5 pour des recommandations concernant les schémas d'évaluation.

4.3.3 Connaissance du laboratoire et de son système de management

Tous les évaluateurs doivent avoir connaissance des éléments suivants:

a) le système de management du laboratoire, y compris les politiques, processus et modes opératoires qui s'appliquent aux évaluateurs;

b) les méthodes approuvées par le laboratoire; et

c) les exigences du laboratoire en matière de compétences.

NOTE La mise en œuvre des systèmes de gestion est très variable. Toutefois, il est fréquent que des éléments tels que le contrôle des documents, des enregistrements, des travaux d'essai et/ou d'étalonnage en cas de non-conformité, le traitement des dossiers techniques et les conflits d'intérêts relèvent de la responsabilité directe des évaluateurs. La plupart des systèmes de management de laboratoire sont fondés sur l'ISO/IEC 17025.

4.4 Connaissance de la sécurité de l'information

Tous les évaluateurs doivent avoir connaissance des éléments suivants:

a) principes de sécurité;

b) propriétés de sécurité;

c) mécanismes d'attaque;

 © ISO/IEC 2018 – Tous droits réservés

d) concepts de potentiel d'attaque;

e) cycle de vie de développement sécurisé;

f) essais de sécurité; et

g) vulnérabilités et faiblesses.

4.5 Connaissance de la technologie évaluée

4.5.1 Connaissance de la technologie évaluée

L'ISO/IEC 15408 (toutes les parties) et l'ISO/IEC 18045 peuvent être utilisées pour l'évaluation d'une grande variété de technologies de l'information. Ces technologies sont souvent classées en différents types de technologies par des schémas d'évaluation, des autorités d'évaluation ou autres.

Tous les évaluateurs doivent avoir connaissance des types de technologies de l'information qu'ils évaluent, y compris les architectures de sécurité communes déployées pour ce type de technologie.

NOTE L'Annexe A fournit une liste informative de sujets de connaissance présentés par des types de technologie couramment identifiés.

EXEMPLE Les types de technologie couramment identifiés comprennent notamment:

— les dispositifs et systèmes de contrôle d'accès;

— le chiffrement, les systèmes de gestion de clés et de PKI (infrastructure de clé publique), les produits pour signatures numériques;

— les bases de données;

— les systèmes d'exploitation;

— les réseaux et les équipements et systèmes liés au réseau;

— les dispositifs et systèmes mobiles;

— les dispositifs multifonctions;

— les circuits intégrés, les cartes à puce et les dispositifs et systèmes liés aux cartes à puce;

— les dispositifs matériels;

— les dispositifs et systèmes de détection; et

— la protection des données, les dispositifs et systèmes biométriques, l'informatique de confiance.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 19896-3:2018
https://standards.iteh.ai/catalog/standards/sist/...-2f33-4ccd-8e89-d462b67840e1/iso-iec-19896-3-2018

4.5.2 Profils de protection, paquets et documents connexes

Tous les évaluateurs doivent avoir connaissance des éléments suivants, lorsqu'ils s'appliquent à la technologie de l'information qu'ils évaluent:

a) les profils de protection, les paquets et tout document de justification connexe spécifié dans le cadre du travail de l'évaluateur;

b) les connaissances requises pour satisfaire à toute méthode d'évaluation et activité d'assurance supplémentaire spécifiée comme étant applicable à une évaluation;

c) la manière de déterminer si des interprétations ou des recommandations concernant les profils de protection, les paquets et les documents de justification connexes ont été publiées et si elles sont applicables à un projet d'évaluation particulier.

© ISO/IEC 2018 – Tous droits réservés