ISO/IEC JTC 1/SC 27

Date: 2023-~~01-23~~02

ISO/IEC 19896-1:2018 (F)

ISO/IEC JTC 1/SC 27

Secrétariat: DIN

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

~~*IT security techniques — Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements*~~

ICS: 35.030

Style Definition: Heading 1: Indent: Left: 0 pt, First line: 0 pt

Style Definition: Heading 2: Font: Bold, Tab stops: Not at 18 pt

Style Definition: Heading 3: Font: Bold

Style Definition: Heading 4: Font: Bold

Style Definition: Heading 5: Font: Bold

Style Definition: Heading 6: Font: Bold

Style Definition: ANNEX

Style Definition: RefNorm

Style Definition: List Number 1

Style Definition: List Continue 1

Style Definition: Body Text_Center

Style Definition: Dimension_100

Style Definition: Figure Graphic

Style Definition: Figure subtitle

Style Definition: AMEND Terms Heading: Font: Bold

Style Definition: AMEND Heading 1 Unnumbered: Font: Bold

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Type de document : **Error! Reference source not found.**
Sous-type de document :
Stade du document : **Error! Reference source not found.**
Langue du document : **Error! Reference source not found.**

Formatted

Formatted: French (Switzerland), Pattern: Clear

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: French (Switzerland)

Formatted: French (Switzerland)

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 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 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).

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 ~~le lien suivant:~~ 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.

Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear

Introduction

La série ISO/IEC 19896 a pour objectif de fournir les concepts fondamentaux concernant la compétence des personnes chargées d'effectuer les évaluations en matière de sécurité des produits informatiques et les essais de conformité. La série ISO/IEC 19896 fournit le cadre et les exigences spécifiques qui définissent la compétence minimale des personnes effectuant des évaluations en matière de sécurité des produits informatiques et les essais de conformité sur la base de normes établies.

Pour atteindre cet objectif, la série ISO/IEC 19896 comprend les éléments suivants~~-~~:

a) les termes et définitions relatifs au thème de la compétence des évaluateurs et des testeurs en matière de sécurité des produits IT~~-~~;

b) les concepts fondamentaux relatifs à la compétence en matière d'évaluation de la sécurité des produits IT et d'essais de conformité~~-~~; et

c) les exigences minimales de compétence pour les évaluateurs et les testeurs en matière de sécurité des produits IT en vue de réaliser les essais/l'évaluation des produits IT.

La série ISO/IEC 19896 présente un intérêt pour~~-~~:

a) les spécialistes de l'évaluation de la sécurité de l'information et des essais de conformité~~-~~;

b) les autorités d'agrément de l'évaluation de la sécurité de l'information et des essais de conformité~~-~~;

c) les laboratoires d'évaluation de la sécurité de l'information et d'essais de conformité~~-~~;

d) les vendeurs ou fournisseurs de technologie dont les produits IT peuvent faire l'objet d'évaluations de l'assurance de la sécurité de l'information ou d'essais de conformité~~-~~;

e) les organismes proposant des certifications ou des reconnaissances professionnelles.

La série ISO/IEC 19896 est organisée en différentes parties afin d'aborder la compétence des professionnels de l'évaluation et des essais comme suit.

Dans le présent document, l'introduction et les concepts donnent une vue d'ensemble des définitions, des concepts fondamentaux et une description générale du cadre utilisé pour communiquer les exigences de compétence pour certains domaines spécialisés. Ce contenu vise à fournir les connaissances fondamentales nécessaires pour utiliser de manière appropriée le cadre présenté dans les autres parties de la série ISO/IEC 19896.

L'ISO/IEC 19896-2 décrit l'ensemble minimal des exigences de compétences à chaque niveau de compétence pour les testeurs de conformité travaillant avec l'ISO/IEC 19790 et les normes associées.

L'ISO/IEC 19896-3 décrit l'ensemble minimal des exigences de compétences à chaque niveau de compétence pour les évaluateurs de la sécurité de l'information travaillant avec l'ISO/IEC 15408 (toutes les parties) et les normes associées.

Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear

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

1 Domaine d'application

Le présent document définit les termes et établit un ensemble structuré de concepts et leurs relations pour comprendre les exigences de compétences des spécialistes des essais de conformité et de l'évaluation pour l'assurance de la sécurité de l'information, établissant ainsi la base d'une compréhension partagée des concepts et des principes centraux de la série ISO/IEC 19896 à travers ses communautés d'utilisateurs. Il fournit des informations fondamentales aux utilisateurs de la série ISO/IEC 19896.

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).

~~<std>ISO/IEC 17000, *Évaluation de la conformité — Vocabulaire et principes généraux*</std>~~

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

ISO/IEC 17000, *Évaluation de la conformité — Vocabulaire et principes généraux*

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 17000 et l'ISO/IEC 17025 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~~l'adresse ~~https://www.iso.org/obp~~https://www.iso.org/obp

— IEC Electropedia~~-~~: disponible à ~~l'adresse~~l'adresse ~~https://www.electropedia.org/~~https://www.electropedia.org/

3.1
compétence
aptitude à mettre en pratique des connaissances et un savoir-faire pour obtenir les résultats escomptés

Formatted: French (Switzerland)
Formatted: French (Switzerland)
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Adjust space between Latin and Asian text, Adjust space between Asian text and numbers

[SOURCE: ISO/IEC 17024:2012, 3.6]

3.2
testeur de conformité
testeur
personne chargée d'effectuer des activités d'essai conformément à une norme d'essai de conformité donnée et à une méthodologie d'essai associée

Note 1 à l'article: L'ISO/IEC 19790 est un exemple d'une telle norme, avec la méthodologie d'essai spécifiée dans l'ISO/IEC 24759.

3.3
instruction
processus consistant à recevoir ou à donner un enseignement systématique, notamment dans une école ou une université

3.4
efficacité
capacité à appliquer les connaissances et les savoir-faire de manière productive, caractérisée par des attributs de comportement tels que l'aptitude, l'initiative, l'enthousiasme, la volonté, les compétences de communication, le travail en équipe et le leadership

3.5
évaluateur
personne chargée d'effectuer des évaluations conformément à une norme d'évaluation donnée et à une méthodologie d'évaluation associée

Note 1 à l'article: L'ISO/IEC 15408 (toutes les parties) est un exemple de norme d'évaluation, avec la méthodologie d'évaluation associée donnée dans l'ISO/IEC 18045.

3.6
expérience
implication pratique dans des projets liés au domaine de compétence

3.7
connaissances
faits, informations, vérités, principes ou compréhension acquis grâce à l'expérience ou à l'instruction

Note 1 à l'article: L'aptitude à décrire les différentes parties d'une norme d'assurance de l'information est un exemple de connaissance.

[SOURCE: ISO/IEC TS 17027:2014, 2.56, modifié — La Note 1 à l'article a été ajoutée.]

3.8
laboratoire
organisme doté d'un système de management fournissant des travaux d'évaluation et/ou d'essai conformément à un ensemble défini de politiques et de modes opératoires et utilisant une méthodologie définie pour soumettre à essai ou évaluer la fonctionnalité de sécurité des produits IT

Note 1 à l'article: Ces organismes se voient souvent attribuer des noms alternatifs par les différentes autorités d'agrément. Par exemple, Centre d'Evaluation de la Sécurité des Technologies de l'Information (CESTI), Common Criteria Testing Laboratory (CCTL), Commercial Evaluation Facility (CLEF).

Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear

3.9
savoir-faire
aptitude à réaliser une tâche ou une activité avec un résultat escompté spécifique, acquise par l'instruction, la formation, l'expérience ou d'autres moyens

Note 1 à l'article: La capacité d'identifier et de classer les risques associés à un projet est un exemple de savoir-faire.

[SOURCE-: ISO/IEC 17027:2014, 2.74, modifié — La Note 1 à l'article a été ajoutée.]

4 Concepts

Un des facteurs permettant d'assurer la conformité de l'évaluation ou des essais de conformité des produits de sécurité des IT est la compétence des personnes qui effectuent les travaux d'évaluation ou d'essai de conformité. Malgré l'existence de méthodes d'essai de conformité ou d'évaluation normalisées, une compétence minimale dans l'exécution des activités nécessaires est requise pour assurer la conformité et la répétabilité des résultats. Cela permet de soutenir la reconnaissance mutuelle des certifications et des validations de l'assurance de la sécurité des produits IT.

L'ISO/IEC 17025 traite des exigences générales relatives à la compétence des laboratoires d'essai et d'étalonnage et est fréquemment spécifiée comme base de conformité parmi les laboratoires d'essai de conformité et d'évaluation de l'assurance de la sécurité.

L'ISO/IEC 17025 identifie plusieurs exigences relatives à la compétence qui doivent être satisfaites par un laboratoire. Il s'agit notamment de-:

— assurer la compétence de tout le personnel pouvant influencer les activités du laboratoire-;

— définir et documenter les exigences en matière de compétence pour chaque fonction impliquée dans les activités du laboratoire-;

— s'assurer que le personnel du laboratoire possède les compétences nécessaires pour réaliser les activités dont il est responsable et qu'il comprend la signification des écarts constatés par rapport aux activités du laboratoire et d'y réagir-;

— disposer d'un processus documenté pour la surveillance continue du personnel impliqué dans les activités de laboratoire-; et

— tenir des registres de compétences tels que le degré d'instruction, la formation, les connaissances techniques, le savoir-faire, l'expérience, les autorisations et la surveillance de tout le personnel impliqué dans les activités de laboratoire.

NOTE L'ISO/IEC 17025 est destinée à couvrir un large éventail de laboratoires d'étalonnage et d'essai et n'est pas uniquement utilisée dans le domaine des essais et de l'évaluation de l'assurance de la sécurité des produits IT.

5 Éléments de compétence

5.1 Compétences

Pour fournir efficacement des résultats d'essais de conformité et d'évaluation cohérents et soutenir l'objectif de conformité des résultats fournis par différentes personnes et différents laboratoires, il est nécessaire que les testeurs de conformité et les évaluateurs aient acquis les connaissances, le savoir-faire,

Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear
Formatted: Pattern: Clear

l'expérience et les qualifications minimales nécessaires en ce qui concerne la norme d'assurance de la sécurité des produits IT visée, et qu'ils soient en mesure d'accomplir leurs fonctions avec efficacité.

Le présent paragraphe définit les éléments minimaux de compétence qu'il convient d'utiliser dans la série ISO/IEC 19896 lors de l'examen des exigences de compétence des testeurs et/ou évaluateurs de conformité pour des normes spécifiques d'assurance de la sécurité des produits IT.

Formatted: Pattern: Clear

Formatted: Pattern: Clear

Une formation peut être fournie afin d'améliorer certains éléments de compétence chez les personnes. Par exemple, la formation est souvent suivie dans le but d'acquérir ou d'améliorer un savoir-faire existant, d'accroître les connaissances ou d'augmenter l'efficacité.

Des éléments de compétence supplémentaires tels que l'aptitude, l'enthousiasme, l'initiative, le leadership, le travail en équipe et la volonté peuvent être spécifiés par les laboratoires ou les organismes d'accréditation. Ils peuvent également être définis dans d'autres parties de la série ISO/IEC 19896.

Formatted: Pattern: Clear

Formatted: Pattern: Clear

5.2 Connaissances

Les connaissances possédées par les testeurs et les évaluateurs sont l'un des éléments de la compétence. Les éléments suivants forment la base de la fourniture d'un corps de connaissance approprié et testable, pertinent pour cette norme d'assurance de la sécurité des produits~~-~~:

a) connaissance de la norme d'assurance de la sécurité de produit IT pertinente~~-~~;

b) toute méthode d'essai ou d'évaluation associée~~-~~;

c) les politiques et modes opératoires des autorités d'agrément, des organismes d'accréditation et des laboratoires pertinents~~-~~; et

d) la connaissance de l'architecture et de la conception des produits IT dans les domaines technologiques pertinents.

En ce qui concerne les produits IT, diverses technologies peuvent être pertinentes pour le domaine d'application d'un laboratoire, et il convient que la connaissance de ces technologies soit prise en compte lors de la définition des niveaux de compétence minimaux. Pour un domaine technologique particulier, les éléments suivants constituent des classes de connaissances pertinentes importantes~~-~~:

a) la technologie utilisée dans la conception, le développement et la mise en œuvre des produits soumis à essai~~-~~;

b) la manière dont les produits sont utilisés ou destinés à être utilisés~~-~~;

c) les vulnérabilités et les faiblesses types qui peuvent se produire avec cette technologie~~-~~; et

d) le domaine dans lequel les produits sont utilisés ou destinés à être utilisés.

La cryptographie, la biométrie, les circuits intégrés, les systèmes d'exploitation, les équipements réseau, les bases de données, les cartes à puce et les systèmes embarqués sont des exemples de domaines technologiques. Les domaines technologiques sont parfois définis, entre autres, par l'autorité d'agrément.

5.3 Savoir-faire

Les savoir-faire généralement exigés des testeurs et des évaluateurs de produits de sécurité IT, selon les niveaux de compétence définis à l'Article 6, incluent notamment les éléments suivants :

Formatted: Pattern: Clear

a) comprendre le domaine d'application et la base d'une évaluation ou d'un projet d'essai de conformité ;

b) comprendre les limites de la mise en œuvre soumise à essai ou de la cible d'évaluation ;

c) être capable de sélectionner ou d'adapter la méthode d'évaluation ou d'essai appropriée ;

d) effectuer une analyse de la documentation ;

e) comprendre le code source, les schémas et les composants de base utilisés pour spécifier et mettre en œuvre les produits ;

f) élaborer et réaliser des essais fonctionnels et non fonctionnels ;

g) déterminer si les conditions d'essai sont conformes aux paramètres indiqués pour permettre la répétabilité des essais ;

h) étalonner et utiliser les outils d'essai ;

i) utiliser un stockage approprié, assurant notamment l'intégrité, la disponibilité et la confidentialité appropriées des preuves d'essai, des résultats d'essai et des enregistrements d'essai, y compris les interprétations et les rapports d'essai ;

j) interpréter les résultats des essais ;

k) être capable de rédiger des rapports compréhensibles détaillant les résultats des travaux ;

l) être capable de répéter un essai, ou de rejouer un essai archivé, puis d'obtenir les mêmes résultats ; et

m) être capable de construire un environnement d'essai en vue d'obtenir un état de fonctionnement approprié pour les produits de sécurité.

À des niveaux de compétence plus élevés, des savoir-faire tels que la capacité à communiquer efficacement et à gérer des projets peuvent également être attendus.

Aux niveaux de compétence 1 et 2, ces savoir-faire peuvent être appliqués sous supervision.

5.4 Expérience

Les personnes expérimentées ont réalisé des évaluations ou des essais de conformité, et ont peut-être enseigné ou encadré d'autres personnes lors de nombreux projets d'essais de conformité ou d'évaluation. Les personnes expérimentées ont une compréhension approfondie des exigences relatives aux projets d'essais de conformité ou d'évaluation, ainsi que des interprétations et des politiques de l'organisme d'accréditation, des autorités d'agrément et des laboratoires.

