SERVICES D'ACCRÉDITATION

Exigences et lignes directrices du CCN relatives à l'accréditation des installations d'évaluation d'essais de produits de sécurité des technologies de l'information

2021-03-19

Conseil canadien des normes

Un monde de possibilités à votre portée.

Canada

Le Conseil canadien des normes
55, rue Metcalfe, bureau 600
Ottawa (Ontario) K1P 6L5

Téléphone : + 1 613 238 3222
Télécopieur : + 1 613 569 7808
accreditation@ccn.ca
www.ccn.ca

Autorisation de reproduction

Also available in English under the title *SCC Requirements and Guidance for the Accreditation of Information Technology Security Evaluation and Testing Facilities*

Table des matières

Avant-propos

Le présent document, intitulé *Exigences et lignes directrices du CCN relatives à l'accréditation des installations d'évaluation et d'essais de produits de sécurité des technologies de l'information*, remplace CAN-P-1591C – *Lignes directrices relatives à l'accréditation des installations d'évaluation et d'essais de produits de sécurité des technologies de l'information (EEPSTI)* (avril 2010).

Le *CAN-P-1621 – Exigences relatives à l'accréditation des installations d'essais de modules cryptographiques et d'algorithmes cryptographiques de novembre 2006* est périmé. Il ne sera pas remplacé vu que le CCN n'offre plus ce programme d'accréditation.

Introduction

Le Centre canadien pour la cybersécurité (CCC), une division du Centre de la sécurité des télécommunications Canada, gère l'organisme de certification (OC) du Schéma canadien d'évaluation et de certification selon les critères communs (SCCC). Le SCCC est un partenariat gouvernement-industrie qui autorise des installations commerciales d'évaluation à mettre à l'épreuve des produits de sécurité des technologies de l'information (STI) selon les Critères communs (CC). Le CCC est chargé d'approuver les Centres d'évaluation selon les CC (CECC); à cette fin, il s'appuie sur leur domaine de spécialité de programme d'évaluation d'essais de produits de sécurité des technologies de l'information (EEPSTI) pour établir leur compétence technique. Les installations d'évaluation dont les compétences sont ainsi reconnues reçoivent un document contenant la portée d'accréditation ci-dessous- celle-ci est propre à la norme des CC.

L'accréditation établit que l'installation possède les compétences et les capacités requises pour effectuer des évaluations et des essais de produits et de systèmes de STI conformément aux normes établies. Ensemble, le CCN et le CCC (l'autorité compétente en matière de STI) offrent une accréditation selon ISO/IEC 17025 aux installations dans leur domaine de spécialité de programme EEPSTI.

Le présent document a pour objet de préciser, lorsqu'il y a lieu, les critères techniques et organisationnels généraux énoncés dans ISO/IEC 17025 aux fins de l'accréditation par le CCN d'installations aptes à évaluer et à mettre à l'essai des produits de STI. Dans leurs domaines d'approbation de STI respectifs, les autorités compétentes en matière de STI peuvent reconnaître l'accréditation des installations pour la conduite des activités énumérées ci-dessous, cette liste n'étant toutefois pas exhaustive :

- l'évaluation de produits et de systèmes en vertu des Critères communs;
- l'examen de produits de STI;
- l'évaluation d'applications de commerce électronique sûr;
- l'évaluation de dispositifs biométriques;
- l'évaluation de la vulnérabilité et les essais de pénétration;

- l’évaluation de dispositifs de sécurité commerciaux spécialisés.

Le Conseil canadien des normes accrédite des laboratoires pour l’exécution d’essais objectifs. Le contrôle de ces essais sera assuré comme suit :

- la constitution d’une documentation sur les essais menés, notamment sur les modalités appliquées;
- la validation des essais;
- la vérification de la formation et des titres de compétences des membres du personnel, et de leur autorisation;
- l’entretien du matériel et des laboratoires.

Et, s’il y a lieu :

- l’étalonnage du matériel;
- l’emploi de matériaux de référence appropriés;
- la prestation de conseils en matière d’interprétation;
- la vérification des résultats;
- l’évaluation des compétences du personnel;
- la consignation de la performance du matériel et des résultats des essais.

1. Références

- ISO/IEC 17025:2017 *Exigences générales concernant la compétence des laboratoires d’étalonnages et d’essais*
- ISO/IEC TR 17026:2015 *Évaluation de la conformité -- Exemple d’un schéma de certification pour des produits tangibles*
- ISO/IEC 15408-1:2009 *Technologies de l’information – Techniques de sécurité – Critères d’évaluation pour la sécurité TI – Partie 1: Introduction et modèle général*
- ISO/IEC 15408-2:2008 *Technologies de l’information – Techniques de sécurité – Critères d’évaluation pour la sécurité TI – Partie 2: Composants fonctionnels de sécurité*
- ISO/IEC 15408-3:2008 *Technologies de l’information – Techniques de sécurité – Critères d’évaluation pour la sécurité TI – Partie 3: Composants d’assurance de sécurité*
- ISO 18045:2008 *Technologies de l’information – Techniques de sécurité – Méthodologie pour l’évaluation de sécurité IT*
- Vocabulaire international de métrologie – Concepts fondamentaux et généraux et termes associés (VIM, 3e édition). JCGM 200:2012 (JCGM 200:2008 avec quelques petites corrections)
- ISO/IEC 17000:2004 *Évaluation de la conformité – Vocabulaire et principes généraux*
- ISO/IEC Guide 2:2004 *Normalisation et activités connexes – Vocabulaire général*
- Aperçu des programmes d’accréditation du CCN

- NIST Handbook 150, NVLAP, Procedures and General Requirements, National Institute of Standards and Technology/National Voluntary Laboratory Accreditation Program (NIST/NVLAP), Gaithersburg, MD USA
- NIST Handbook 150-20 Checklist, Information Technology Security Testing Common Criteria

2. Définitions

Les définitions applicables aux fins du présent document englobent toutes les définitions d'ISO/IEC 17025:2017 (p. ex., laboratoire, laboratoire d'essais, laboratoire d'étalonnage, étalonnage, essais, méthode d'étalonnage, méthode d'essai, vérification, système qualité, manuel qualité, étalon de référence, matériau de référence, matériau de référence certifié, traçabilité, essai d'aptitude, exigences d'accréditation) et les définitions pertinentes d'ISO/IEC 17000 (p. ex., assurance qualité, maîtrise de la qualité), ainsi que les définitions ci-dessous qui sont propres au présent document.

Signataires approuvés : Personnes qualifiées et autorisées à signer le rapport d'essai ou le certificat d'étalonnage avant sa remise au client.

Approbation : Détermination par une autorité en matière de sécurité de l'information du fait qu'une installation possède dans un domaine d'activité précis les compétences techniques requises pour effectuer l'évaluation et l'essai de produits de STI; autorisation officielle habilitant l'installation à mener des essais dans le contexte de l'EEPSTI.

Conception fonctionnelle : Caractéristiques conceptuelles de la structure et caractéristiques de fonctionnement du produit de STI.

Évaluation : Analyse et essais de conformité menés en fonction de critères nationaux et internationaux d'évaluation de la sécurité (p. ex., les Critères communs). Au CCN, ce terme est l'équivalent d'« essai ».

Installation d'évaluation et d'essais de produits de STI (EEPSTI) : Dans le contexte des services d'accréditation du CCN, installation accréditée par le CCN dans le cadre du domaine de spécialité de programme EEPSTI, pour effectuer des évaluations et des essais de produits de STI.

Installation : Organisme effectuant des évaluations et des essais de sécurité. Lorsque l'installation fait partie d'une organisation menant des activités supplémentaires autres que l'évaluation et les essais, le terme « installation » se rapporte exclusivement aux divisions de ladite organisation qui participent au processus d'évaluation.

Accréditation d'une installation : Reconnaissance officielle de la conformité d'une installation aux exigences d'accréditation en matière d'EEPSTI. L'accréditation d'une installation établit que

l'installation possède les compétences et les capacités requises pour effectuer des évaluations et des essais de produits et de systèmes de STI conformément aux exigences en matière d'EEPSTI.

Domaine d'approbation de STI : Domaine spécialisé de la STI pour lequel il existe une autorité compétente reconnue, et pour lequel :

a) des normes ont été établies (ou le seront) pour la conduite d'activités spécialisées d'évaluation et d'essais de STI;
b) il existe un besoin en matière d'évaluation de produits ou de services de STI;
c) les compétences individuelles ou organisationnelles nécessaires pour mener à bien les évaluations et les essais de sécurité spécialisés sont reconnues;
d) il existe une exigence de maîtrise et de surveillance d'une gamme précise d'essais et d'évaluation de produits STI;
e) il existe un besoin en matière de révision et d'approbation des résultats des évaluations et des essais;
f) il existe une ou des installations d'EEPSTI accréditées par le CCN.

Sécurité des technologies de l'information : Tout ce qui se rapporte à la définition, à la mise en œuvre et à la préservation de la confidentialité, de l'intégrité, de la disponibilité, de l'imputabilité et du contrôle d'accès.

Personnel technique clé : Personnel de l'installation possédant les pouvoirs nécessaires pour prendre les décisions techniques importantes en matière d'évaluation. Le « chef », le « responsable » et le « chef d'équipe » chargé des évaluations en sont des exemples.

Évaluation sur place : Examen sur place d'une installation en vue d'évaluer sa conformité aux conditions et aux critères d'accréditation relatifs à l'EEPSTI.

Produit : Toute technologie de sécurité de TI destinée à assurer la protection des biens et qui fait l'objet d'activités d'évaluation et d'essais de sécurité. Ces technologies peuvent comprendre aussi bien des composants matériels ou logiciels autonomes que des systèmes entièrement intégrés, et peuvent englober toutes les procédures qui assurent l'utilisation sûre de ces technologies dans l'environnement auquel elles sont destinées.

Essais d'aptitude : Démonstration par une installation de sa capacité d'effectuer des essais et des évaluations applicables à sa portée d'accréditation. Dans le cadre de l'EEPSTI, les installations sont tenues de démontrer leurs compétences théoriques et pratiques en ce qui concerne l'exécution d'évaluations et d'essais de produits de STI.

Enregistrements : Données étayées, conservées pour référence ultérieure, portant sur une intervention, une analyse, un résultat ou un événement particulier ou toute autre activité particulière se rapportant à l'évaluation et à l'essai de produits de STI. Les enregistrements doivent être conservés sous une forme appropriée (électronique ou autre) et permanente

pendant leur durée de vie utile telle que définie par l'autorité compétente reconnue en matière de STI.

Autorité compétente reconnue en matière de STI : Organisation qui exerce un rôle directeur, une autorité officielle ou une influence directe sur un domaine d'approbation de STI afin de vérifier la conformité aux normes et aux pratiques exemplaires appropriées en matière d'évaluation et d'essai dans le domaine de compétence visé. Cette organisation est responsable de l'approbation des installations d'EEPSTI accréditées pour la conduite d'activités spécialisées d'évaluations et d'essais en vue de l'approbation ou de la certification des résultats relatifs aux produits dans les domaines d'approbation visés.

Exigences de sécurité : Spécifications relatives à la fonctionnalité ou aux caractéristiques conceptuelles d'un produit de technologie de l'information qui, lorsqu'elles sont intégrées au produit, contribuent à assurer la sécurité.

Examen technique : Processus par lequel une équipe d'évaluation rattachée à une installation d'EEPSTI acquiert une connaissance suffisante d'un produit pour pouvoir porter un jugement technique sur sa capacité de satisfaire à une exigence de sécurité particulière.

Outils d'essai : Désigne tous les équipements, y compris le matériel, les logiciels, les utilitaires et les procédures connexes, employés à l'appui des activités d'évaluation et d'essais de produits de sécurité. L'équipement devrait convenir aux emplois prévus et être géré, utilisé et entretenu conformément aux exigences du fabricant et à toutes autres pratiques appropriées.

Validation: La validation d'un outil ou d'une procédure d'essai est le processus qui consiste à vérifier, dans la mesure où cela est possible, que l'outil fonctionnera adéquatement ou que la procédure produira des résultats conformes aux spécifications des séries d'essais pertinentes, des normes pertinentes ou de versions antérieurement validées d'outils d'essais.

3. Portée des essais

3.1 Les activités d'EEPSTI englobent aussi bien des essais menant à des résultats catégoriques, comme les essais de pénétration de garde-barrières, les vérifications de résistance des mots de passe ou les taux de fausse acceptation des dispositifs biométriques, que des activités pouvant comporter une bonne part d'interprétation, comme l'évaluation de la robustesse des fonctions et des caractéristiques de sécurité d'un produit logiciel ou matériel STI.

3.2 L'EEPSTI consiste en l'analyse des caractéristiques d'un produit logiciel ou matériel STI qui visent à assurer les services de sécurité suivants :

- la confidentialité de l'information;
- l'intégralité de l'information;
- la disponibilité;

- la reddition de compte.

3.3 Les caractéristiques de sécurité qui peuvent être mises à l'essai englobent, sans s'y limiter, les aspects suivants :

- les fonctions d'identification et d'authentification;
- les audits de sécurité (constitution et stockage sécurisé de pistes d'audit, analyse des événements relatifs à la sécurité);
- les fonctions de non-répudiation;
- les fonctions cryptographiques (opérations cryptographiques, gestion des clés cryptographiques);
- la transmission sécurisée de données (implantation et application du contrôle de l'accès ou des règles ou politiques de flux de données);
- l'intégralité des données stockées;
- la gestion des fonctions de sécurité, des données relatives à la sécurité et des rôles de gestion de la sécurité;
- la protection des fonctions de sécurité, notamment l'impossibilité de contournement et l'isolation de domaines;
- l'utilisation des ressources (résilience, priorité de service, attribution des ressources);
- les fonctions à sécurité intégrée;
- les fonctions d'autotest;
- la protection physique (détection/prévention des sabotages).

3.4 Les techniques employées pour évaluer les caractéristiques de sécurité englobent, sans s'y limiter, les aspects suivants :

- l'auto-examen avec résultats connus;
- l'analyse de la vulnérabilité afin de s'assurer que le client a envisagé toutes les vulnérabilités éventuelles du produit STI évalué;
- l'examen des codes logiciels;
- l'analyse approfondie de l'environnement de conception et de la documentation connexe en vue de déterminer l'efficacité du système de gestion des configurations applicable au produit STI évalué;
- l'examen approfondi de la documentation de livraison pour établir si elle décrit bien toutes les procédures requises pour préserver l'intégrité du produit STI évalué;
- l'examen et mise à l'essai des procédures d'installation, de génération et de démarrage pour déterminer si elles sont complètes et assez détaillées pour permettre une configuration sécurisée du produit STI évalué;
- l'analyse approfondie de la documentation de conception, notamment les spécifications fonctionnelles, la conception de haut niveau et la conception de bas niveau, afin de confirmer qu'elle instancie correctement toutes les interfaces et toutes les fonctions de sécurité inhérentes au produit évalué;
- l'analyse approfondie des guides d'utilisation et d'administration afin d'établir s'ils expliquent bien et sans ambiguïté comment se servir du produit et l'administrer de

manière sécuritaire et s'ils sont conformes à toute autre documentation fournie aux fins de l'évaluation;

- l'examen et évaluation, dans le cadre de visites sur place, des procédures de sécurité à l'égard de la conception afin de déterminer si elles exposent de manière assez précise les mesures nécessaires dans l'environnement de conception pour assurer la confidentialité et l'intégrité du concept et de l'implantation du produit STI;
- l'analyse des essais des clients en vue d'en établir la couverture et la profondeur, et réalisation d'essais de fonctionnement et de pénétration indépendants;
- la mise en correspondance des politiques de sécurité;
- le traçage des exigences de sécurité.

3.5 Approche générale en matière d'essais STI

3.5.1 La méthodologie appliquée distingue quatre principaux volets de la planification et l'exécution des essais liés à l'évaluation de la sécurité d'installations d'EEPSTI : l'analyse de la couverture des essais, les plans d'essais, les procédures d'essais et les résultats d'essais.

3.5.2 L'analyse de la couverture des essais met habituellement en correspondance les caractéristiques de sécurité et les résultats des essais qui démontrent le fonctionnement adéquat des fonctions de sécurité. Elle peut servir à prouver que toutes les caractéristiques de sécurité ont été mises à l'essai.

3.5.3 Le plan d'essai précise la mesure dans laquelle chaque caractéristique de sécurité sera mise à l'essai, l'approche adoptée à cette fin ainsi que les ressources nécessaires, notamment en fait d'équipements, de personnel et de temps, pour réaliser les essais de la façon indiquée.

3.5.4 La procédure d'essai décrit la marche à suivre, conformément au plan d'essai, pour mettre en place le contexte nécessaire à la conduite des essais, réunir les conditions voulues, procéder aux essais et documenter les résultats projetés. Elle doit être consignée de façon suffisamment détaillée pour éviter toute ambiguïté au cours des essais et pour permettre à d'autres évaluateurs de la reprendre ultérieurement et d'obtenir les mêmes résultats.

3.5.5 Les résultats d'un essai attestent les résultats réels observés au cours d'un essai et doivent être consignés de façon suffisamment détaillée pour permettre la comparaison avec les résultats projetés et pour faciliter les comparaisons si le même essai est répété ultérieurement. Les résultats réels obtenus permettent de prendre une décision concernant la protection assurée.

4. Équipe d’évaluation

4.1 Composition de l’équipe d’évaluation

4.1.1 Le CCN fournit l’évaluateur principal pour chaque accréditation ou réévaluation; le CCC fournit au moins un évaluateur technique pour les évaluations sur place et les essais d’aptitude.

4.2 Préparation de l’évaluation sur place

4.2.1 L’évaluation sur place vise à faciliter la démonstration de la conformité du fonctionnement d’une installation à la norme ISO/IEC 17025.

4.2.2 Avant de procéder à l’évaluation sur place, les évaluateurs examineront le manuel qualité de l’installation et le curriculum vitæ des membres du personnel. S’ils ont besoin d’autres documents à l’appui d’un essai d’aptitude, ils doivent en informer l’installation avant l’évaluation pour qu’elle puisse les lui remettre.

4.3 Essais d’aptitude

Consulter l’annexe B.

ANNEXE A: Application des exigences d'ISO/IEC 17025:2017 aux installations d'EEPSTI

Chaque application vise à préciser les exigences générales énoncées dans ISO/IEC 17025:2017 pour lesquelles les critères d'essais et d'évaluation expressément applicables à l'EEPSTI seront utilisés. Le tableau ci-dessous indique les numéros des articles d'ISO/IEC 17025:2017 visés par chaque application.

ISO/IEC 17025:2017 Section :	Notes sur l'application des exigences aux installations d'EEPSTI
4. Exigences générales	
4.1.1 4.1.4	• l'installation peut, à la discrétion de l'autorité compétente en matière de STI, concevoir des produits STI; et • l'installation peut, à la discrétion de l'autorité compétente en matière de STI, fournir des services de consultation en vue d'essais STI d'un tel produit et participer à ces essais. • les risques compromettant l'impartialité qui découlent des démarchées mentionnées seront cernés et mitigés.
5. Exigences structurelles	
5.4	Lorsque des essais sont menés dans les locaux d'un client ou à hors de l'installation, toutes les exigences d'EEPSTI applicables aux équipements, aux aménagements et à l'environnement s'appliqueront.
6. Exigences relatives aux ressources	
6.2.2	• Au moins un membre du personnel technique de l'installation est tenu d'assumer des fonctions de gestion de posséder une vaste expérience de la STI. En ce qui concerne les installations qui sont des Centres d'évaluation selon les Critères communs, la formation et l'expérience en STI du personnel seront passées en revue et analysées en fonction d'une grille de compétences prédéfinie élaborée par l'autorité compétente reconnue en matière de STI. • L'installation est tenue de compter, parmi son personnel technique, au moins trois employés ayant une formation appropriée (un diplôme universitaire ou collégial en informatique, en génie ou dans une discipline connexe, ou une certification professionnelle) et une vaste expérience pertinente de la modélisation des menaces, de l'analyse de l'architecture de sécurité, des essais de pénétration ou en évaluation de produits de sécurité.

6.2.5	Le système de management doit contenir des renseignements sur les politiques et les procédures (programme de formation) qui régissent la vérification périodique des compétences de tout le personnel prenant part à la conduite et à l'évaluation des essais. Si un seul membre du personnel de l'installation possède les compétences nécessaires pour être responsable d'un aspect spécifique des essais, les audits doivent au moins comprendre une revue de la documentation et des instructions ainsi qu'une vérification du respect des procédures et des instructions, et de la documentation présentant les résultats d'essais.
6.3.1	L'espace dont dispose l'installation pour les évaluations STI doit être entretenu de manière à permettre ces évaluations. Cette exigence s'applique aux locaux aménagés pour l'évaluation et l'essai de produits de sécurité, la formation du personnel, la tenue des enregistrements ou la conservation des documents, des logiciels ou du matériel informatique.
6.3.4	Doivent être en place des procédures pour séparer les aspects logistiques des différentes évaluations durant le stade essai. Il s'agit notamment d'assurer que les équipements, les services et les serveurs soient consacrés à l'évaluation d'un produit en particulier. Mentionnons la numérisation et la segmentation des réseaux informatiques comme exemples de méthodes pour bien délimiter les processus d'évaluation.
6.4.1	Pour mener à bien les activités couvertes par la portée d'accréditation, l'installation est tenue de disposer des équipements matériels et logiciels, ainsi que des installations informatiques, appropriés pour mener des évaluations et des essais de produits STI. Elle doit être pourvue de systèmes convenables sur place à l'appui des évaluations de sécurité qui sont adaptés aux essais visés par la demande d'accréditation. L'installation doit avoir ou être en mesure de fournir, sur préavis raisonnable, l'infrastructure de TI nécessaire aux fonctions suivantes : • le traitement de textes pour la production de rapports; • la communication sécurisée par courriel avec les clients, l'autorité compétente en matière de STI, etc.; • l'accès à Internet; • l'utilisation de tout outil spécialisé requis dans le cadre du travail d'évaluation.
6.4.3	Aux fins de l'EEPSTI, le terme « équipements » désigne les produits matériels et logiciels et tout autre mécanisme d'évaluation utilisés

	par l'installation à l'appui de l'évaluation et de la mise en essai d'un produit STI. L'installation doit se doter de systèmes appropriés à l'appui d'évaluations et d'essais de produits STI sur le terrain. Les équipements utilisés pour les essais doivent être employés et entretenus : • conformément aux recommandations du fabricant; et • tel qu'indiqué dans la méthode d'essai; ou • selon les exigences détaillées propres au domaine de spécialité EEPSTI. L'installation doit avoir des procédures qui encadrent la configuration des essais et des différents produits de TI y afférents. Ces procédures peuvent se décliner en PON particulières ou peuvent être intégrées au plan d'essai de chaque évaluation. L'installation est tenue d'avoir des procédures visant à assurer la conservation, l'élimination ou le retour appropriés des logiciels et du matériel informatique après la conclusion de l'évaluation.
6.4.12	Pour limiter les risques que posent les pirates et leurs maliciels, l'installation doit veiller à la protection des équipements logiciels en appliquant les rustines nécessaires et en renforçant la sécurité au besoin.
7. Exigences relatives au processus	
7.1.1	L'installation d'EEPSTI et son client sont tenus de s'entendre par écrit sur ce qui constitue la cible des essais et l'environnement dans lequel la cible sera testée. Il s'agit notamment de définir le produit particulier mis en essai, la configuration adoptée aux fins des essais et l'environnement externe dans lequel ceux-ci se dérouleront. L'installation d'EEPSTI et le client sont tenus de s'entendre par écrit sur les éléments suivants : • le produit particulier mis à l'essai; • la configuration adoptée aux fins des essais; • les lieux où seront effectués les essais ou l'évaluation; • tout appui à la préparation de l'environnement d'évaluation fournie par le client, tel que l'envoi d'équipements spécialisés sur les lieux des essais et l'installation d'un système d'exploitation ou de bases de données particuliers, etc.; • les documents à livrer par le client;

	• les documents à livrer par l'installation; • les méthodes d'essai qu'utilise l'installation. Les rapports d'essais définitifs doivent être conservés par l'installation pour la période prévue par le client ou l'autorité compétente en matière de STI.
7.4.1	L'installation est tenue d'avoir des procédures concernant : • la manipulation et l'intégralité des produits; • la manipulation et l'intégralité des outils et des logiciels d'essais; • l'exécution d'essais sur place.
7.5.1	L'installation est tenue d'utiliser et d'entretenir un système de maîtrise des enregistrements fonctionnel afin d'assurer le suivi des activités liées aux essais pour chaque évaluation de produit de sécurité. Les enregistrements associés aux activités d'évaluation doivent être traçables aux normes et aux méthodes reconnues de l'industrie, s'il y a lieu. Les enregistrements doivent être facilement accessibles et contenir des données suffisantes pour permettre à une entité indépendante de déterminer quel travail d'évaluation a été effectivement accompli et de confirmer les constatations. L'installation d'EEPSTI est également tenue de conserver des enregistrements sur les éléments suivants : • l'établissement et la modification de procédures et de méthodologies d'évaluation; • l'approbation ou le rejet de produits soumis à une évaluation; • le suivi complet des multiples versions des données d'évaluation et des rapports techniques d'évaluation; • le suivi complet des activités d'évaluation, y compris l'analyse initiale, les verdicts et tout changement subséquent à ces derniers (p. ex., à la suite de la modification de preuves ou d'une analyse additionnelle); • les informations nécessaires pour reproduire tout essai mené durant une évaluation; • la configuration de tout équipement d'essai employé durant une évaluation et l'analyse de ces équipements visant à confirmer s'ils conviennent à l'exécution des essais voulus. L'installation est tenue de conserver, de divulguer et de détruire ses enregistrements conformément à sa politique à l'égard des renseignements exclusifs de nature confidentielle ainsi qu'aux engagements contractuels conclus avec ses clients.

7.8.1.2	L’installation d’EEPSTI est tenue de publier des rapports d’essais qui présentent de façon exacte, claire et non ambiguë les conditions d’essais, la configuration d’essais, les résultats des essais et toute l’information requise.
7.8.3.1 e)	Chaque rapport d’essai doit indiquer les types d’essais standard effectués ou fournir une description des essais.
8. Exigences relatives au système de management	
8.4.2	L’installation doit être dotée d’un système de sauvegarde efficace afin de pouvoir récupérer toutes données d’évaluation (ou enregistrements) éventuellement perdues.

ANNEXE B: Portée d'accréditation des centres d'évaluation selons les critères communs

Introduction

L'accréditation établit qu'une installation dispose des compétences et des capacités voulues pour exécuter des évaluations et des essais de produits et de systèmes de sécurité des technologies de l'information (STI). La présente annexe liste les méthodes d'évaluation et d'essais spécifiques que les installations peuvent employer selon la norme ISO/IEC 15408 (aussi appelée Critères communs, ou CC) à l'aide du document méthodologique ISO/IEC 18045 (aussi appelé méthodologie d'évaluation commune, ou CEM).

La présente annexe fait aussi état des compétences que doivent posséder le personnel de l'installation, ainsi que des méthodes d'essai propres aux CCEC.

Portée d'accréditation

Selon les normes suivantes :

- ISO/IEC 15408-1:2009 Critères d'évaluation pour la sécurité TI - Partie 1 : Introduction et modèle général
- ISO/IEC 15408-2:2008 Critères d'évaluation pour la sécurité TI - Partie 2: Exigences fonctionnelles de sécurité
- ISO/IEC 15408-3:2008, Critères d'évaluation pour la sécurité TI - Partie 3 : Exigences d'assurance de sécurité
- ISO/IEC 18045:2008 Technologies de l'information - Techniques de sécurité – Méthodologie pour l'évaluation de sécurité TI

La portée d'accréditation inclut les activités d'évaluation et d'essais suivantes :

- APE : évaluation de profils de protection;
- ASE : évaluation d'une cible de sécurité;
- EAL1 : premier niveau d'assurance de l'évaluation;
- EAL2 : deuxième niveau d'assurance de l'évaluation;
- ALC_FLR : correction d'anomalies;
- Profils de protections approuvés par le CCS.

Compétences et habiletés requises

Pour les besoins de la portée d'accréditation, présentée ci-dessus, le personnel de l'installation est tenu d'avoir une connaissance fonctionnelle des normes ISO/IEC 15408 et ISO/IEC 18045 et de posséder les compétences et les habiletés nécessaires pour réaliser selon les exigences des deux normes les activités suivantes :

- évaluer un profil de protection;

- évaluer une cible de sécurité;
- effectuer une analyse approfondie de l'environnement de conception du client et de la documentation connexe en vue de déterminer l'efficacité du système de gestion des configurations du client;
- effectuer un examen approfondi de la documentation de livraison du client afin d'établir si cette dernière décrit bien toutes les procédures requises pour préserver l'intégralité du produit STI évalué;
- examiner et mettre à l'essai les procédures d'installation, de génération et de démarrage pour déterminer si elles sont complètes et assez détaillées pour permettre une configuration sécurisée du produit STI évalué;
- effectuer une analyse approfondie de la documentation de conception, notamment les spécifications fonctionnelles, la conception de haut niveau et de bas niveau, afin de confirmer qu'elle instancie correctement toutes les interfaces et toutes les fonctions de sécurité inhérentes au produit évalué;
- analyser en profondeur les guides d'utilisation et d'administration afin d'établir s'ils expliquent clairement la façon d'utiliser le produit et de l'administrer de manière sécuritaire et s'ils sont conformes à toute autre documentation fournie aux fins de l'évaluation;
- examiner et évaluer, au cours de visites sur place, les procédures de sécurité à l'égard de la conception afin de déterminer si elles font une description suffisamment détaillée des mesures de sécurité nécessaires dans l'environnement de conception pour assurer la confidentialité et l'intégrité du concept et de l'implantation du produit STI;
- faire une analyse de la vulnérabilité pour vérifier si le client a envisagé toutes les vulnérabilités éventuelles du produit STI en question;
- évaluer les essais conçus par des clients en vue d'en établir la portée et la rigueur, et mener des essais de fonctionnement et de pénétration indépendants;
- passer en revue le plan d'essai, l'approche d'essai, les procédures d'essais et les résultats d'essais du client, et étudier les données d'essais afin de démontrer que les fonctions de sécurité sont conformes aux spécifications et ont été systématiquement éprouvées par rapport aux spécifications fonctionnelles et à la conception de haut niveau;
- concevoir des essais de fonctionnement par suite de l'analyse de la documentation de conception, des guides et de la documentation des essais du client, de l'exécution d'un vaste échantillon des scénarios d'essais du client et de la création de scénarios d'essais complémentaires;
- concevoir des essais de pénétration fondés sur une analyse de la vulnérabilité, les spécifications fonctionnelles, la conception de haut niveau, la conception de bas niveau et les guides d'installation;
- rendre compte des observations, des évaluations et des essais conformément aux exigences du SCCC.

Essais d’aptitude – Processus de contrôle technique

Comme nous l’avons mentionné plus haut, il incombe à l’OC d’assurer la surveillance technique des travaux d’évaluation selon les CC réalisés par les CCEC. Grâce à ce processus, l’OC peut déterminer si un CECC réalise des évaluations de qualité ou si celui-ci doit prendre des mesures correctives. Pour se conformer aux Schéma canadien d’évaluation et de certification selon les Critères communs (SCCC), l’installation doit être en mesure de mener les activités suivantes :

- déposer une soumission d’admissibilité indiquant clairement le produit TI à mettre à l’épreuve et la portée logistique des fonctionnalités de sécurité, et qui évalue aussi les éventuelles applications des profils de protection pertinents pour ce genre de produit;
- effectuer les activités d’évaluation conformément aux exigences des CC et de la CEM, et produire les données d’évaluation pour l’OC pendant l’évaluation proprement dite;
- répondre aux rapports d’observation formulés par l’OC;
- préparer un rapport technique d’évaluation (RTE) dans lequel sont consignées les constatations;
- travailler en équipe pour mener l’évaluation.

L’OC peut choisir d’observer certaines activités d’évaluation plus attentivement ou de répéter des activités d’évaluation plus que d’habitude au cours d’autres évaluations selon les CC, afin de vérifier que les analyses et les procédures appropriées sont bel et bien appliquées. Les résultats du processus de surveillance technique décrit ci-dessus peuvent servir aux fins des essais d’aptitude.

Outre le processus de surveillance technique, l’OC évalue, met à l’essai et approuve les candidats aux postes d’évaluateur selon les CC. Pour participer aux activités d’évaluation à ce titre, les membres du personnel doivent montrer qu’ils ont suivi la formation et acquis l’expérience pertinente en STI, ainsi que réussir un examen de l’OC qui met à l’épreuve leurs connaissances et leurs habiletés dans l’application des CC et de la CEM. L’OC remet aux personnes ayant satisfait à ces deux exigences un certificat d’évaluateur qui précise leur compétence dans le cadre du SCCC.

Le CCN considère que le cadre sur les essais de produits présenté plus haut est conforme aux exigences de la disposition 7.7.2 de la norme ISO/IEC 17025:2017.