Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Exigences et procédures relatives au Programme canadien lié aux Critères communs pour les laboratoires d'essais

POUR LES LABORATOIRES D'ESSAIS

TLP:WHITE

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

1
9743476

Canada

AVANT-PROPOS

La présente publication intitulée *Exigences et procédures relatives au Programme canadien lié aux Critères communs pour les laboratoires d'essais* est un document NON CLASSIFIÉ. Elle remplace le document *Schéma canadien lié aux Critères communs Guide nº 3 : Approbation des installations d'évaluation, version 3.0, août 2016*.

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le 1er avril 2020.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1.0	Publication initiale	Août 2004
2.0	Mise à jour majeure visant à refléter la nouvelle structure adoptée pour les guides, les instructions et les procédures fonctionnelles du Programme lié aux Critères communs.	Septembre 2010
3.0	Mise à jour de la matrice des compétences en annexe et ajout de la section *Signature de l'entente*.	Août 2016
4.0	Reformatage du modèle de document pour le Centre canadien pour la cybersécurité et mise à jour de la description de certains changements apportés aux processus.	Avril 2020

VUE D'ENSEMBLE

L'objet du présent document est de décrire les exigences et le processus par lequel une organisation commerciale (ci-après appelée l'« entreprise ») peut devenir un centre d'évaluation selon les Critères communs (ci-après appelé le « laboratoire d'essais ») approuvé fonctionnant en vertu du Programme canadien lié aux Critères communs.

Il est destiné aux entreprises qui veulent devenir un laboratoire d'essais dans le cadre du Programme canadien. Les commanditaires de l'évaluation (généralement des fournisseurs), les développeurs et les consommateurs peuvent également consulter le présent document pour obtenir de l'information utile sur les exigences relatives aux laboratoires d'essais fonctionnant en vertu du Programme canadien.

TABLE DES MATIÈRES

LISTE DES ANNEXES

1 INTRODUCTION

Dans le cadre du Programme canadien lié aux Critères communs, les organisations commerciales exploitent des laboratoires d'évaluation selon les Critères communs (ci-après appelés les « laboratoires d'essais ») et procèdent aux évaluations de sécurité des produits de technologies de l'information (TI).

Le présent document décrit les exigences et procédures relatives au Programme canadien lié aux Critères communs pour les laboratoires d'essais fonctionnant en vertu du Programme canadien. Il comprend le processus qu'une organisation commerciale (ci-après appelée l' « entreprise ») peut suivre pour devenir un laboratoire d'essais approuvé.

1.1 À PROPOS DU PROGRAMME CANADIEN LIÉ AUX CRITÈRES COMMUNS

Le Centre canadien pour la cybersécurité (ci-après appelé le Centre pour la cybersécurité) gère le Programme canadien lié aux Critères communs et agit à titre d'organisme de certification. Le Centre pour la cybersécurité est le signataire canadien de l'*Arrangement relatif à la reconnaissance des certificats liés aux Critères communs dans le domaine de la sécurité des TI* [1] communément appelé l'Arrangement de reconnaissance des Critères communs (ARCC) ci-après. Pour de plus amples renseignements sur le fonctionnement du programme canadien, prière de consulter le *Manuel de qualité du Programme canadien lié aux Critères communs* [2].

REMARQUE : Un laboratoire d'essais participant au programme canadien peut également porter le nom de l'ARCC (laboratoire agréé) ou le nom officiel de la certification du Conseil canadien des normes (CCN) (installation d'évaluation et essais de produits de sécurité des technologies de l'information [EEPSTI]).

2 EXIGENCES RELATIVES AUX LABORATOIRES D'ESSAIS

Cette section traite des exigences auxquelles l'entreprise doit se conformer pour devenir un laboratoire d'essais approuvé.

2.1 ACCRÉDITATION D'INSTALLATION EEPSTI

Ces exigences visent à s'assurer que les laboratoires d'essais fonctionnent conformément aux prescriptions du Guide ISO/IEC 17025, *Exigences générales concernant la compétence des laboratoires d'étalonnage et d'essais* [3].

2.1.1. L'entreprise doit détenir une accréditation d'installation d'évaluation et essais de produits de sécurité des technologies de l'information (EEPSTI) valide délivrée par le Conseil canadien des normes [4].

Le Conseil canadien des normes et le Centre pour la cybersécurité examineront attentivement la capacité de l'entreprise de satisfaire à toutes les exigences du Guide ISO/IEC 17025 dans le cadre de cette accréditation.

2.2 EXIGENCES RELATIVES AUX CONFLITS D'INTÉRÊTS

Ces exigences visent à s'assurer que l'entreprise effectuera tous les travaux d'évaluation sans influence indue au sein de l'installation ou en provenance de l'extérieur.

2.2.1. L'entreprise doit disposer de procédures appropriées pour s'assurer que les membres de sa direction n'exercent pas d'influence indue sur les résultats des activités d'évaluation selon les CC.

2.2.2. Si l'entreprise est contrôlée par une société mère, l'installation doit démontrer qu'il y a une séparation suffisante des contrôles et des influences, de sorte que les membres de sa direction :

- n'exercent pas d'influence indue sur les résultats des activités d'évaluation selon les CC;
- ne puissent pas accéder de façon inappropriée aux renseignements exclusifs utilisés pendant l'évaluation.

2.2.3. L'entreprise doit avoir mis en place des procédures appropriées pour s'assurer qu'il n'y a pas de conflit d'intérêts entre (1) le personnel qui donne des conseils pour aider un commanditaire à se préparer à l'évaluation de son produit de TI, et (2) le personnel qui effectue l'évaluation selon les CC à proprement dite.

2.2.4. L'entreprise informera le Centre pour la cybersécurité dans les dix jours ouvrables suivant tout changement de propriétaire ou de tout changement lié à la gestion de l'entreprise.

2.3 EXIGENCES EN MATIÈRE DE SÉCURITÉ

Ces exigences visent à s'assurer que l'entreprise est en mesure de protéger les renseignements sensibles.

2.3.1. L'entreprise doit disposer d'une *vérification d'organisation désignée* selon la définition donnée dans le *Manuel de la sécurité industrielle* de Services publics et Approvisionnement Canada (SPAC) [5]. Tout le personnel de l'installation doit à tout le moins avoir fait l'objet d'une vérification approfondie de la fiabilité par SPAC.

2.4 EXIGENCES RELATIVES À L'INSTALLATION PHYSIQUE

Ces exigences visent à s'assurer que l'entreprise relève de la compétence du Programme canadien lié aux Critères communs.

2.4.1. L'entreprise doit maintenir une installation physique permanente au Canada et avoir accès à un bureau et à de l'équipement suffisants pour accueillir au moins un membre du Centre pour la cybersécurité qui assurera le contrôle technique des évaluations au besoin.

2.4.2. L'entreprise doit disposer, ou pouvoir se doter dans un délai raisonnable, d'une infrastructure de TI suffisante pour appuyer toutes les fonctions de l'évaluateur.

2.5 EXIGENCES RELATIVES AU PERSONNEL

Ces exigences visent à s'assurer que l'entreprise a le personnel qualifié nécessaire pour procéder à l'évaluation selon les Critères communs.

2.5.1. Au moins trois membres du personnel de l'entreprise doivent posséder un certificat d'évaluateur délivré par le Centre pour la cybersécurité.

2.5.2. Au moins un membre du personnel doit satisfaire les exigences relatives à la désignation d'évaluateur en chef ci-dessous :

- se trouver au Canada;
- avoir assumé le rôle d'évaluateur des CC pendant au moins six mois au cours des deux années précédentes, dans le cadre d'un programme d'autorisation de certificat de l'ARCC avec lequel le Centre pour la cybersécurité a un haut niveau de familiarité.

2.5.3. Lorsqu'un évaluateur des Critères communs qualifié quitte le laboratoire d'essais, l'entreprise doit en informer le Centre pour la cybersécurité dans les dix jours ouvrables suivant son départ.

2.6 COMPÉTENCE TECHNIQUE

Ces exigences visent à s'assurer que l'entreprise a les compétences techniques nécessaires pour procéder à l'évaluation selon les Critères communs.

2.6.1. L'entreprise doit réussir un essai d'évaluation (voir la section 3.4) pour un produit de TI approuvé du Centre pour la cybersécurité et effectuer les activités d'évaluation conformément aux exigences stipulées dans les *Instructions du Programme canadien lié aux Critères communs* [6], les *Critères communs pour l'évaluation de la sécurité des technologies de l'information* [7], la *Common Methodology for Information Security Evaluation* [8] et un ou plusieurs profils de protection [9].

2.6.2. L'entreprise procédera à toutes les évaluations selon les normes de qualité exigées par le Centre pour la cybersécurité.

3 PROCÉDURES POUR LES LABORATOIRES D'ESSAIS

3.1 DEVENIR UN LABORATOIRE D'ESSAIS

La présente section décrit les étapes qu'une entreprise doit suivre pour devenir un laboratoire d'essais agréé.

1. L'entreprise s'assure qu'elle respecte les exigences stipulées à la section 2.
2. Elle doit communiquer avec le Centre pour la cybersécurité à l'adresse contact@cyber.gc.ca pour faire part de son intérêt à devenir un laboratoire d'essais et fournir les renseignements suivants :
    a. Nom légal complet de l'entreprise;
    b. Emplacement du laboratoire d'essais;
    c. Coordonnées du point de contact principal;

    Le Centre pour la cybersécurité confirmera s'il accepte de nouvelles demandes pour devenir un laboratoire d'essais.
3. L'entreprise démontre qu'elle satisfait toutes les exigences relatives aux laboratoires d'essais stipulées à la section 2 :
    a. Communiquer avec le Conseil canadien des normes pour obtenir une accréditation ISO/IEC 17025 avec une portée d'EEPSTI;
    b. S'adresser au Centre pour la cybersécurité pour les autres exigences.
4. L'entreprise établit une entente officielle avec le Centre pour la cybersécurité afin de devenir un laboratoire d'essais agréé.

3.2 MAINTENIR UN LABORATOIRE D'ESSAIS

Les entreprises doivent continuer de répondre à toutes les exigences pour conserver le statut de laboratoire d'essais approuvé. L'approbation accordée à l'entreprise pour servir de laboratoire d'essais pourrait être révoquée si ce dernier ne satisfait pas à toutes les exigences ou n'arrive pas à remédier aux lacunes relevées par le Centre pour la cybersécurité.

Le Centre pour la cybersécurité pourrait révoquer l'approbation d'une entreprise dans les circonstances suivantes :

- L'entreprise ne répond pas aux exigences relatives aux laboratoires d'essais et n'a pas remédié aux lacunes relevées par le Centre pour la cybersécurité dans les délais indiqués par le Centre pour la cybersécurité;
- L'entreprise nuit à la réputation du Programme canadien lié aux Critères communs, soit par un piètre rendement dans le cadre de ses évaluations, ou par le non-respect des règles du Programme canadien lié aux Critères communs, y compris la mauvaise utilisation des logos associés au Programme canadien lié aux Critères communs ou à l'ARCC.

3.3 QUALIFICATION DES ÉVALUATEURS DE CRITÈRES COMMUNS

Le Centre pour la cybersécurité exige que tous les évaluateurs soient titulaires d'un certificat d'évaluateur. Pour obtenir un certificat d'évaluateur, les candidats doivent faire ce qui suit :

1. obtenir 9 points ou plus dans la matrice des compétences de l'évaluateur (voir l'annexe A);
2. obtenir une note de 66 % à l'examen d'évaluateur.

Les certificats délivrés aux évaluateurs ne sont pas transférés automatiquement d'un laboratoire d'essais à l'autre si les évaluateurs changent d'entreprise. Si un candidat est déjà détenteur d'un certificat d'évaluateur, le Centre pour la cybersécurité pourrait décider de reconnaître la qualification précédente selon l'historique du candidat en matière d'évaluation et le délai écoulé depuis la plus récente évaluation des Critères communs réalisée par le candidat.

Pour obtenir des certificats d'évaluateur, une entreprise doit fournir au Centre pour la cybersécurité un curriculum vitæ récent et une matrice des compétences de l'évaluateur dûment remplie (voir l'annexe A) pour chacun des candidats. Le Centre pour la cybersécurité procédera à la validation de la matrice des compétences des évaluateurs et offrira aux candidats retenus l'occasion de passer un examen écrit. Cet examen vise à tester les connaissances du candidat sur les Critères communs, la méthodologie d'évaluation commune et les profils de protection courants.

Le Centre pour la cybersécurité s'attend à ce que les candidats possèdent de solides connaissances pratiques du sujet avant de passer l'examen d'évaluateur. Avant chaque examen, le Centre pour la cybersécurité offre un atelier d'une demi-journée, qui met l'accent sur la structure et les exigences de la méthodologie d'évaluation commune et des Critères communs, aborde certains des profils de protection courants et propose des détails précis sur les exigences et procédures relatives au Programme canadien lié aux Critères communs.

Les certificats d'évaluateur seront délivrés aux candidats en fonction de leurs résultats à l'examen. Les candidats ayant obtenu une note de 66 % ou plus obtiendront un certificat d'évaluateur. Les candidats ayant obtenu entre 60 % et 65 % deviendront des évaluateurs apprentis, tandis que ceux dont la note est inférieure à 60 % devront reprendre l'examen.

Les évaluateurs apprentis peuvent obtenir un certificat d'évaluateur en démontrant leur capacité à réaliser des évaluations des Critères communs dans la pratique. Il incombe au laboratoire d'essais de créer un plan d'apprentissage pour les évaluateurs apprentis et de le soumettre au Centre pour la cybersécurité aux fins d'examen. L'entreprise fait le point régulièrement avec le Centre pour la cybersécurité sur les progrès réalisés par le candidat, et le Centre pour la cybersécurité détermine quand l'évaluateur apprenti est prêt à obtenir un certificat d'évaluateur.

3.4 EFFECTUER UNE ÉVALUATION D'ESSAI

L'objectif de l'évaluation d'essai est de démontrer que l'entreprise peut se conformer à l'exigence 2.6.1. L'évaluation d'essai offre également aux membres du personnel l'occasion de se conformer à l'exigence de l'évaluateur en chef (exigence 2.5.2). Cette évaluation d'essai met également fin à l'essai de compétence qui compose l'accréditation EESTI (exigence 2.1.1).

Dans le cadre de l'évaluation d'essai, l'entreprise évalue un produit de TI que le Centre pour la cybersécurité juge adéquat. Le produit de TI doit respecter les exigences d'admissibilité énoncées dans les *Instructions du Programme canadien lié aux Critères communs* [6] et le Centre pour la cybersécurité s'assurera que la portée des fonctions de sécurité du produit en question est suffisante pour que l'entreprise puisse démontrer sa capacité d'évaluation. L'entreprise gère tous les arrangements commerciaux avec le commanditaire de l'évaluation réalisée à titre d'essai.

Au cours de l'évaluation d'essai, le Centre pour la cybersécurité examinera certaines activités de façon plus détaillée que lors des évaluations des Critères communs régulières. Le Centre pour la cybersécurité évaluera la capacité de l'entreprise à effectuer ce qui suit :

- réaliser les activités d'évaluation conformément aux *Instructions du Programme canadien lié aux Critères communs* [6], aux *Critères communs pour l'évaluation de la sécurité* [7], à la *Common Methodology for Information Security Evaluation* [8] et aux profils de protection [9], le cas échéant;
- produire une preuve d'évaluation (dont des rapports d'observation) pendant l'évaluation;
- répondre aux rapports d'observation formulés par le Centre pour la cybersécurité;
- préparer un rapport technique d'évaluation pour consigner les constatations;
- travailler de façon coordonnée en équipe afin de réussir l'évaluation.

S'il estime que l'entreprise a réalisé une évaluation de qualité élevée, le Centre pour la cybersécurité ajoutera l'évaluation réalisée à titre d'essai à la liste des produits certifiés publiée sur le portail international des Critères communs. Dans l'évaluation du rendement de l'entreprise, le Centre pour la cybersécurité tiendra compte du fait que l'évaluation d'essai constitue probablement une expérience d'apprentissage pour l'entreprise.

Si l'évaluation d'essai ne peut être achevée en raison de l'incapacité du produit de TI ou du commanditaire de l'évaluation de satisfaire aux exigences liées aux Critères communs, le Centre pour la cybersécurité peut exiger que l'entreprise procède à une autre évaluation d'essai. L'admissibilité à la deuxième évaluation d'essai reposera sur la facilité avec laquelle le Centre

pour la cybersécurité a été en mesure d'observer les diverses activités d'évaluation effectuées par l'entreprise et d'interagir avec elle.

Si le rendement de l'entreprise est jugé insatisfaisant, le Centre pour la cybersécurité refusera d'approuver sa demande pour en faire un laboratoire d'essais.

4 CONTENU COMPLÉMENTAIRE

4.1 LISTE DES ABRÉVIATIONS

Terme	Définition
ARCC	Arrangement relatif à la reconnaissance des certificats liés aux Critères communs
ISO/IEC	Organisation internationale de normalisation (*International Organization for Standardization*) / Commission électrotechnique internationale (*International Electrotechnical Commission*)
TI	Technologies de l'information
EEPSTI	Évaluation et essais de produits de sécurité des technologies de l'information
SPAC	Services publics et Approvisionnement Canada
CCN	Conseil canadien des normes

4.2 RÉFÉRENCES

Numéro	Référence
[1]	Critères communs. *Arrangement relatif à la reconnaissance des certificats liés aux Critères communs dans le domaine de la sécurité des TI*. Disponible au https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf.
[2]	Centre de la sécurité des télécommunications. *Manuel de qualité du Programme canadien lié aux Critères communs*. Disponible au https://www.cyber.gc.ca/fr/orientation/programme-canadien-lie-aux-criteres-communs-manuel-de-qualite.
[3]	ISO/IEC 17025: *General requirements for the competence of testing and calibration laboratories*
[4]	Conseil canadien des normes. *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.* Disponible au https://www.scc.ca/fr/notre-organisme/publications/exigences-et-procedures-accreditation/exigences-et-lignes-directrices-du-ccn-relatives-a-laccreditation-des-installations-devaluation-et
[5]	Services publics et Approvisionnement Canada (SPAC). *Manuel de la sécurité industrielle*. Disponible au https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/index-fra.html
[6]	Centre de la sécurité des télécommunications. *Instructions du Programme canadien lié aux Critères communs.* Disponible au https://cyber.gc.ca/fr/orientation/instructions-du-programme-canadien-lie-aux-criteres-communs.
[7]	Critères communs. *Common Criteria for Information Technology Security Evaluation*. Disponible au https://commoncriteriaportal.org/cc/.
[8]	Critères communs. *Common Methodology for Information Technology Security Evaluation*. Disponible au https://commoncriteriaportal.org/cc/.
[9]	Critères communs. *Protection profiles*. Disponible au https://www.commoncriteriaportal.org/pps/.

Annexe A Matrice des compétences de l'évaluateur

Les évaluateurs du Centre pour la cybersécurité feront appel à l'outil d'évaluation retrouvé dans cette annexe pour évaluer les curriculum vitæ des candidats.

Description	Description	Note
Familier	• La personne a lu les ouvrages de base sur le sujet.	0
Connaissances opérationnelles	• La personne a travaillé au moins à un projet d'une durée minimale de quatre mois, et a démontré ses compétences à un superviseur. • Cette expérience peut avoir été acquise sur une grande période dans le cadre d'un projet en milieu universitaire.	1
Connaissances exhaustives	• La personne a appliqué ses compétences et ses connaissances pendant au moins deux ans, dans un milieu non universitaire. • Expérience acquise pendant des études de maîtrise ou de doctorat, accordé au cas par cas.	2
Connaissances d'expert	• La personne est reconnue dans l'industrie comme un expert dans son domaine. • Elle a publié des ouvrages spécialisés et/ou a collaboré à la rédaction de tels ouvrages, a présenté des cours, etc.	3

REMARQUES :

- Le Centre pour la cybersécurité ne considère pas que les compétences ou l'expérience acquises en tant que superviseur ou gestionnaire sont pertinentes aux fonctions que l'évaluateur sera appelé à assumer. Les détails devraient être liés de façon directe à l'expérience dans un rôle technique, sans supervision.
- Les candidats devraient considérer le temps réellement consacré à une activité au moment d'estimer la durée de leur expérience de travail dans chaque catégorie.

A.1 Renseignements sur le candidat

Date	
Nom du candidat	
Laboratoire d'essais	

A.2 Formation officielle

Catégorie	Description	Note
Diplôme ou certificat		
Note totale pour la formation officielle (maximum de 3 points)		

REMARQUE : Sélectionnez la catégorie qui accorde le plus grand nombre de points parmi les scénarios suivants :

- Certificat d'études collégiales : 1 point pour un certificat technologique ou technique applicable;
- Baccalauréat : 2 points pour un baccalauréat d'une université agréée en informatique, en génie électrique ou dans un domaine scientifique applicable;
- Maîtrise ou doctorat : 3 points pour une maîtrise ou un doctorat d'une université agréée en informatique, en génie électrique ou dans un domaine scientifique applicable.

A.3 Expérience en matière d'essais

Catégorie	Description	Durée	Note
Essais du système : comprend les tests au niveau du réseau et les tests d'interopérabilité de différents produits de TI interconnectés			
Essais de produits de TI : vérification des options et débogage			
Essais de conformité : tests des produits de TI par rapport à des normes définies			
Essais de vulnérabilité : essais de produits ou de réseaux en fonction des vulnérabilités en matière de sécurité			
Cours : p. ex. outils de tests automatisés, techniques pratiques de tests de logiciels			
Note totale pour l'expérience en matière d'essais (maximum de 4 points)			

A.4 Connaissance en sécurité des TI

Catégorie	Description	Durée	Note
Politiques et procédures de sécurité des TI : rédaction, élaboration et mise en œuvre			
Évaluation des menaces et des risques : exécution et rédaction d'EMR, choix des mesures de protection			
Sécurité de réseau : SDI, RPV, murs coupe-feu, etc.			
Sécurité des communications : sans fil, cellulaires, etc.			
Cryptographie : algorithmes, protocoles, FIPS 140			
Normes de sécurité des TI : rédaction, mise en œuvre, intégration			
Qualifications professionnelles : (p. ex. CISSP)			
Cours de sécurité des TI : (décrire chacun des cours)			
Note totale pour la connaissance en sécurité des TI (maximum de 5 points)			

A.5 Développement de produits

Catégorie	Description	Durée	Note
Conception : rédaction de spécifications fonctionnelles et de conception détaillée			
Programmation : codage des composants, modules, modification des caractéristiques			
Contrôle de version : utilisation des outils de version, procédures de mise en œuvre			
Cours : (p. ex. langages de programmation, techniques de développement logiciel)			
Note totale pour le développement de produits (maximum de 3 points)			

A.6 Note globale

Points totaux accordés au candidat (maximum de 15 points)	