Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Programme canadien lié aux Critères communs

Manuel qualité

POUR LES PRATICIENS DES CRITÈRES COMMUNS

TLP:WHITE

Canada

AVANT-PROPOS

Le présent document intitulé *Programme canadien lié aux Critères communs* : *Manuel qualité* est une publication NON CLASSIFIÉ. Ce document remplace le *Programme canadien lié aux Critères communs* : *Manuel qualité version 4.0, mars 2020*.

DATE D'ENTRÉE EN VIGUEUR

La présente publication entre en vigueur le 15 juin 2022.

HISTORIQUE DES RÉVISIONS

Révision	Modifications	Date
1.0	Première diffusion publique	Août 2004
2.0	Mise à jour majeure reflétant une structure révisée pour les guides, les instructions et les procédures fonctionnelles du Programme lié aux Critères communs	Septembre 2010
3.0	Modification des processus d'admissibilité des évaluations et d'acceptation des évaluations.	Août 2016
3.1	Fusion des sections décrivant les approches de gestion des documents et des dossiers. Mise à jour de la section sur l'examen périodique des activités.	Octobre 2016
4.0	Révision importante pour mieux harmoniser le document avec les exigences de l'Arrangement de reconnaissance des Critères communs et les pratiques de publication du Centre pour la cybersécurité.	Mars 2020
4.1	Plusieurs modifications de contenu	Juin 2022

APERÇU

Le présent document est le « Manuel qualité » du Programme canadien lié aux Critères communs administré par le Centre canadien pour la cybersécurité. Il décrit l'organisme et les politiques du programme visant à satisfaire aux obligations internationales de l'*Arrangement relatif à la reconnaissance des certificats liés aux Critères communs dans le domaine de la sécurité des technologies de l'information*.

TABLE DES MATIÈRES

1 Introduction 4
2 Organisme de certification 6
3 Personnel de l'organisme de certification 9
4 Activités de l'organisme de certification 14
5 Plaintes, différends et appels 19
6 Utilisation des certificats, DES marques et DES logos de certification 22
7 Contenu complémentaire 23

LISTE DES FIGURES

Figure 1 Organigramme de l'organisme de certification 9

1 INTRODUCTION

Le présent document décrit le fonctionnement du Programme canadien lié aux Critères communs, un programme de test des technologies de l'information (TI) fondé sur la norme internationale *Critères communs pour l'évaluation de la sécurité des technologies de l'information* (en anglais seulement), aussi appelés Critères communs ou CC), qui permet aux laboratoires de test autorisés d'évaluer la cybersécurité des produits de TI. Les utilisateurs de produits de TI peuvent accroître de degré de fiabilité de leurs mécanismes de cybersécurité lorsqu'ils ont recours aux produits assujettis aux évaluations de produits selon les Critères communs.

Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité) est l'une des directions du Centre de la sécurité des télécommunications (CST). Il gère et applique le Programme canadien lié aux Critères communs et agit à titre d'organisme de certification; il encadre les évaluations effectuées par les installations commerciales d'évaluation de la sécurité des TI (ci-après désignés par le terme « laboratoire de test ») pour en assurer la qualité.

Le CST est mandaté par gouvernement du Canada pour agir à titre de signataire de l'*Arrangement international relatif à la reconnaissance des certificats liés aux Critères communs dans le domaine de la sécurité des technologies de l'information (ARCC)* (en anglais seulement), qui établit un cadre international de reconnaissance mutuelle des résultats des évaluations réalisées selon les Critères communs dans les pays participants.

D'autres pays signataires de l'Arrangement de reconnaissance des critères communs (ARCC) reconnaissent les certificats de produits canadiens liés aux Critères communs. Ce processus de reconnaissance mutuelle permet à un fournisseur de faire évaluer ses produits de TI dans un laboratoire de test du pays de son choix, plutôt que de passer de multiples évaluations redondantes dans plusieurs pays.

1.1 PUBLIC CIBLE

Le présent document s'adresse premièrement au personnel de l'organisme de certification, qui a la responsabilité directe de veiller à la qualité suivant les normes du programme canadien. Deuxièmement, il s'adresse aux laboratoires de test et aux commanditaires des évaluations (fournisseurs), car ils ont un intérêt direct dans le succès des certifications, et il peut être à leur avantage de bien comprendre les procédures mises en place par l'organisme de certification pour assurer la qualité. Ce document pourrait également s'adresser aux utilisateurs de produits de sécurité des TI, ainsi qu'aux autres signataires de l'ARCC.

1.2 POLITIQUES DÉTERMINANTES

Le présent document satisfait aux exigences de l'ARCC concernant les organismes de certification.

1.3 SURVOL DU DOCUMENT

Le présent document compte les parties suivantes :

- la section 2, qui décrit l'organisme de certification;
- la section 3, qui décrit l'organisme de l'organisme de certification et son personnel;

- la section 4, qui décrit les activités de l'organisme de certification;
- la section 5, qui décrit comment l'organisme de certification résout les différends avec les participants;
- la section 6, qui décrit comment l'organisme de certification protège la marque des Critères communs.

2 ORGANISME DE CERTIFICATION

2.1 APERÇU

C'est le Centre pour la cybersécurité qui pourvoit le personnel de l'organisme de certification. Ainsi, tous les membres du personnel de l'organisme de certification sont des employés du gouvernement du Canada et sont donc assujettis aux politiques, règles et règlements applicables du gouvernement du Canada, y compris ceux qui traitent de la protection des renseignements sensibles et des conflits d'intérêts. Dans le cadre de son rôle d'organisme de certification, le Centre pour la cybersécurité remplit plusieurs fonctions, notamment les suivantes :

- l'approbation des laboratoires de test aux fins du programme canadien;
- la qualification des évaluateurs dans les laboratoires de test;
- le contrôle technique des évaluations;
- la délivrance et le retrait des certificats liés aux Critères communs;
- la production des rapports de certification;
- la production des rapports de maintien de l'assurance;
- la tenue d'une liste de produits certifiés pour les évaluations réalisées dans le cadre du programme canadien;
- la représentation du Canada à titre de signataire de l'ARCC.

2.2 STATUT JURIDIQUE ET POUVOIRS

Le Centre pour la cybersécurité est une direction du Centre de la sécurité des télécommunications (CST), un ministère du gouvernement du Canada qui, en vertu de la *Loi sur le Centre de la sécurité des télécommunications*, agit à titre d'autorité technique nationale en matière de cybersécurité et d'assurance de l'information. Le gouvernement du Canada fournit le financement nécessaire au fonctionnement du Programme lié aux Critères communs suivant la responsabilité du Centre pour la cybersécurité qui est, notamment, de fournir des services contribuant à la protection de l'information électronique et des infrastructures d'information, principalement celles des institutions fédérales canadiennes et celles qui sont désignées comme étant importantes par le ministre du CST.

2.3 COMMUNICATION AVEC L'ORGANISME DE CERTIFICATION

Le Centre pour la cybersécurité administre le Programme canadien lié aux Critères communs, et la principale personne-ressource pour les demandes de renseignements externes est le superviseur du Programme lié aux Critères communs. En outre, les lecteurs peuvent communiquer avec le programme comme suit :

Par la poste:

Critères communs
Centre canadien pour la cybersécurité
Case postale 9703,
Terminal
Ottawa (Ontario) K1G 3Z4
Canada

Par courrier électronique :

contact@cyber.gc.ca

2.4 POLITIQUE DE MAINTIEN DE LA QUALITÉ

Le Centre pour la cybersécurité s'engage à veiller à ce que son personnel mène toutes les activités de l'organisme de certification conformément aux normes exigées par l'ARCC. Le Centre pour la cybersécurité s'attend à ce que tous les employés s'acquittent de leurs fonctions avec intégrité, impartialité et objectivité conformément aux politiques et aux procédures énoncées dans le système de gestion de la qualité.

Le Centre pour la cybersécurité effectue régulièrement des examens organisationnels afin d'évaluer l'efficacité du système de gestion de la qualité et de déterminer les aspects à améliorer sur le plan des activités et des procédures de l'organisme de certification.

2.5 FRAIS DE CERTIFICATION

Le Centre pour la cybersécurité veille à ce que ses services soient disponibles sans condition financière excessive en ne facturant pas ses services de certification selon les Critères communs.

2.6 POLITIQUE DE NON-DISCRIMINATION

Le Centre pour la cybersécurité assure le fonctionnement et l'administration non discriminatoires des services et des fonctions de l'organisme de certification, et n'impose aux demandeurs aucune condition financière (ou autre) qui soit excessive.

2.7 IMPARTIALITÉ, VALEURS ET ÉTHIQUE

Tous les membres du personnel de l'organisme de certification doivent exécuter les tâches qui leur sont attribuées d'une manière impartiale, objective et équitable. En tant qu'employés du CST, tous les membres du personnel de l'organisme de

certification sont assujettis à la Charte d'éthique du CST, qui comprend des lignes directrices sur les conflits d'intérêts qui répondent à l'exigence C.2 de l'ARCC.

2.8 EXAMEN PÉRIODIQUE DES ACTIVITÉS

Le Centre pour la cybersécurité effectue des examens périodiques de toutes les activités de l'organisme de certification. Ces examens visent à l'évaluer l'efficacité et la pertinence des politiques et procédures de l'organisme de certification, et à déterminer si l'organisme de certification continue de répondre aux exigences du gouvernement du Canada et de partager les objectifs de l'ARCC.

3 PERSONNEL DE L'ORGANISME DE CERTIFICATION

3.1 ORGANISME

Le Programme canadien lié aux Critères communs comporte les rôles suivants :

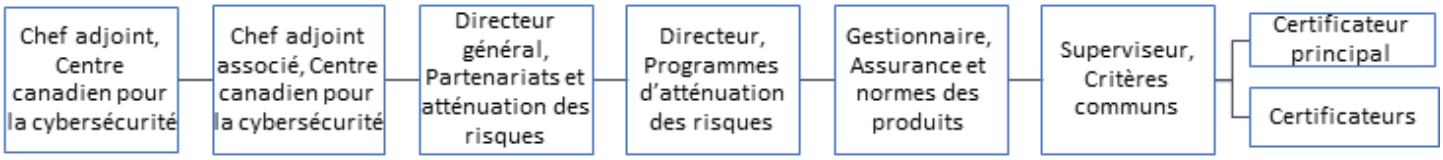

Figure 1 Organigramme de l'organisme de certification

3.2 RÔLES ET RESPONSABILITÉS

Pour veiller à ce que le personnel s'acquitte de ses tâches de manière efficace et efficiente, le présent document définit les responsabilités, les études minimales, l'expérience et les connaissances pertinentes exigées du personnel de l'organisme de certification.

3.2.1 TOUT LE PERSONNEL DE L'ORGANISME DE CERTIFICATION

Tous les membres du personnel de l'organisme de certification doivent suivre les directives fournies dans la documentation de l'organisme de certification. Le personnel doit s'assurer que le superviseur des Critères communs est au courant de toute lacune ou erreur dans la documentation du système de gestion de la qualité.

3.2.2 DIRECTEUR, PROGRAMMES D'ATTÉNUATION DES RISQUES

Le directeur, Programmes d'atténuation des risques dirige l'organisme de certification; il est aussi le cadre supérieur responsable de la participation du Canada au programme international de l'ARCC. L'organigramme dans la section 3.1 montre la structure hiérarchique du directeur, Programmes d'atténuation des risques, aux cadres supérieurs du Centre canadien pour la cybersécurité. Le directeur est responsable de ce qui suit :

- Approuver l'orientation stratégique du programme;
- Approuver les opérations et les activités du programme.

3.2.3 GESTIONNAIRE, ASSURANCE ET NORMES DES PRODUITS

Le gestionnaire, Assurance et normes des produits, est l'autorité qui délivre les certificats pour le programme et est responsable du déroulement efficace et efficient des activités. Il est chargé notamment de ce qui suit :

- Communiquer l'orientation stratégique au superviseur du programme;
- Superviser les activités de gestion de programme exercées par le superviseur du programme;
- Assurer l'évolution du système de gestion de la qualité;

- Représenter le Canada à l'occasion au Comité international de gestion de l'ARCC;
- Traiter les plaintes, les différends et les appels au sein de l'organisme de certification.

Ce rôle exige des connaissances poussées dans le domaine des TI et de la sécurité des TI, lesquelles doivent être acquises suivant une combinaison d'études formelles et d'expérience pertinente.

3.2.4 SUPERVISEUR, CRITÈRES COMMUNS

Le superviseur, Critères communs (ci-après désigné comme étant « le superviseur ») tient les rôles de gestionnaire opérationnel et de gestionnaire de la qualité pour le programme. Le superviseur est responsable de ce qui suit :

- Exercer les tâches qui incombent au gestionnaire opérationnel et au gestionnaire de la qualité pour le programme;
- Agir à titre de point de liaison principal pour les questions d'ordre technique et non technique;
- Transmettre les directives techniques et administratives au personnel :
    - veiller à ce que le personnel de l'organisme de certification comprenne son rôle et ses responsabilités,
    - définir les exigences pour le contrôle technique des évaluations,
    - s'assurer que le document relatif aux méthodes d'évaluation et de certification est exact et à jour;
- Gérer les activités quotidiennes de certification du programme :
    - accepter de nouvelles évaluations dans le programme,
    - affecter les équipes de certification aux évaluations,
    - approuver les rapports de certification;
- Surveiller le rendement et le fonctionnement du système de gestion de la qualité :
    - signaler les problèmes en remontant la chaîne de gestion,
    - effectuer des examens périodiques,
    - mettre en œuvre les changements découlant de l'examen interne ou externe,
    - assurer le suivi de tous les rapports de non-conformité,
    - veiller à ce que des mesures correctives et préventives soient prises au besoin;
- Superviser les activités du laboratoire de test :
    - valider les connaissances et l'expérience des candidats-évaluateurs, pour évaluer leur admissibilité à passer l'examen d'évaluateur,
    - classer les examens des évaluateurs,
    - affecter des évaluateurs techniques qualifiés pour assister le Conseil canadien des normes (CCN) aux fins d'accréditation des laboratoires de test;
- Examiner périodiquement l'efficacité des politiques, des lignes directrices et des procédures existantes, puis créer ou perfectionner des approches, le cas échéant;
- Agir à titre de principale personne-ressource chargée de suivre les plaintes, les différends et les appels jusqu'au terme de leur traitement;

- Représenter le programme au sein de comités internationaux de l'ARCC, notamment le conseil de développement, le sous-comité exécutif et le comité de gestion.

Ce rôle exige ce qui suit :

- Diplôme universitaire ou collégial en science informatique, en génie informatique/électrique ou en mathématiques, ou encore connaissances équivalentes acquises dans le cadre d'une expérience professionnelle pertinente;
- Vaste connaissance des théories et principes de la sécurité des TI, de l'évaluation de la sécurité informatique et des méthodes de certification;
- Expérience poussée avec les Critères communs et la Méthodologie d'évaluation commune des produits de sécurité des technologies de l'information (CEM) acquise en participant directement à son élaboration et/ou à son application;
- Expérience des rapports avec les fournisseurs, les consultants, et les organismes et partenaires internationaux.

3.2.5 CERTIFICATEUR

Le certificateur est principalement responsable de ce qui suit :

- Signaler tout conflit d'intérêts lié aux évaluations dont il est responsable auprès du superviseur;
- Effectuer le contrôle technique des évaluations effectuées par les laboratoires de test :
    - assurer la qualité technique des résultats et la conformité aux Critères communs, à la CEM ou aux profils de protection,
    - évaluer la qualité des activités d'évaluation,
    - observer les activités d'évaluation réalisées par le laboratoire de test,
    - évaluer la documentation fournie par le laboratoire de test,
    - fournir une orientation technique aux laboratoires de test pour résoudre les problèmes;
- Effectuer le contrôle technique des demandes de maintien de l'assurance;
- Produire des rapports de certification et des rapports de maintenance;
- Aider les certificateurs principaux à effectuer les tâches nécessaires à l'approbation des nouveaux laboratoires de test;
- Exercer un contrôle technique et de l'aide pendant la réévaluation des laboratoires de test par le CCN.

Ce rôle exige ce qui suit :

- Diplôme universitaire ou collégial en science informatique, en génie informatique/électrique ou en mathématiques, ou encore connaissances équivalentes acquises dans le cadre d'une expérience professionnelle pertinente;
- Connaissance des théories et principes de la sécurité des TI, de l'évaluation de la sécurité informatique et des méthodes de certification.

3.2.6 CERTIFICATEUR PRINCIPAL

Le certificateur principal est responsable de ce qui suit :

- Toutes les activités d'un certificateur;
- Veiller à ce que les méthodes techniques du programme soient adéquates et uniformes;
- Produire des interprétations des Critères communs, de la CEM et des profils de protection;
- Conseiller le superviseur sur tous les aspects techniques du programme, y compris l'efficacité des politiques, des lignes directrices et des procédures;
- Fournir des conseils et des avis aux certificateurs au sujet de la gestion des certifications, ainsi que de l'application et de l'interprétation des Critères communs, de la CEM et du profil de protection;
- Effectuer les tâches nécessaires à l'approbation des nouveaux laboratoires de test,
    - offrir des séances de formation aux candidats au poste d'évaluateur;
    - élaborer les examens d'évaluateur de Critères communs et les faire passer aux candidats;
- Participer aux comités de l'ARCC international.

Ce rôle exige ce qui suit :

- Diplôme universitaire ou collégial en science informatique, génie informatique/électrique ou en mathématiques, ou connaissances équivalentes acquises dans le cadre d'une expérience professionnelle pertinente;
- Vaste connaissance des théories et principes de la sécurité des TI, de l'évaluation de la sécurité informatique et des méthodes de certification;
- Expérience significative avec les Critères communs et la CEM, acquise par la participation directe à l'élaboration et/ou à l'application des Critères communs et/ou de la CEM.

3.3 EXIGENCES EN MATIÈRE DE FORMATION

Le Centre pour la cybersécurité suit les procédures de recrutement et de dotation du gouvernement du Canada lorsqu'il pourvoit des postes vacants au sein de l'organisme de certification, afin d'assurer l'embauche des membres du personnel les plus aptes pour l'organisme de certification. Le Centre pour la cybersécurité considère que tout membre du personnel de l'organisme de certification qui ne possède pas les qualifications minimales décrites dans les sections précédentes est considéré comme étant en formation. Le superviseur encadre et surveille étroitement le rendement de tout le personnel en formation.

Le Centre pour la cybersécurité tient à jour des renseignements sur les qualifications, la formation et l'expérience pertinentes de tous les membres du personnel de l'organisme de certification dans ses systèmes ministériels de planification des ressources et de gestion de l'information, conformément aux processus du gouvernement du Canada en matière de gestion des ressources humaines.

Le Centre pour la cybersécurité reconnaît que les certificateurs peuvent acquérir des compétences et des connaissances grâce à une combinaison de cours de formation structurée, de programmes d'autoapprentissage et de formation pratique supervisée. Les membres du personnel de l'organisme de certification doivent avoir un plan de formation personnalisé pour assurer leur perfectionnement continu et font l'objet d'évaluations annuelles du rendement.

3.4 ENTREPRENEURS

L'organisme de certification n'emploie pas actuellement d'entrepreneurs pour l'exécution des tâches normales. Si le Centre pour la cybersécurité devait faire appel à des entrepreneurs, ceux-ci se conformeraient à toutes les politiques et procédures du programme canadien, et seraient l'objet d'un encadrement rigoureux visant à assurer le respect de ces politiques et procédures ainsi que la qualité de leur travail.

4 ACTIVITÉS DE L'ORGANISME DE CERTIFICATION

Dans les sections suivantes, nous décrivons brièvement les activités menées par le Centre pour la cybersécurité, et nous indiquons les mesures instaurées pour assurer la qualité.

4.1 APPROBATION DES NOUVEAUX LABORATOIRES DE TEST

Le Centre pour la cybersécurité doit approuver officiellement un laboratoire de test avant qu'il puisse effectuer des évaluations dans le cadre du Programme canadien lié aux Critères communs. Veuillez consulter le *Exigences et procédures relatives au Programme canadien lié aux Critères communs pour les laboratoires d'essais* pour obtenir de plus amples renseignements sur l'approbation des laboratoires de test.

Le Centre pour la cybersécurité et chacun des laboratoires de test signent conjointement une entente officielle qui englobe toutes les procédures pertinentes, y compris les dispositions visant à assurer la confidentialité des renseignements protégés et les processus d'évaluation et de certification.

4.2 ACCEPTATION DES ÉVALUATIONS

Le Centre pour la cybersécurité examine les produits conformément aux *Instructions du Programme canadien lié aux Critères communs*. Il est à noter qu'une fois l'évaluation acceptée, le promoteur de l'évaluation peut demander une entente de non-divulgation avec le Centre pour la cybersécurité.

4.3 DÉSIGNATION DE CERTIFICATEURS

Lorsqu'il affecte un certificateur à une évaluation, le superviseur tient compte de plusieurs facteurs, notamment les suivants :

- Connaissance approfondie des Critères communs, de la CEM et des profils de protection applicables;
- Connaissances de technologies particulières;
- Possibilités de formation des certificateurs;
- Considérations relatives aux conflits d'intérêts.

Plus précisément, les certificateurs ne doivent pas avoir d'intérêt particulier dans le succès ou l'échec de la certification, conformément aux lignes directrices en matière d'éthique du gouvernement du Canada. Par conséquent, les certificateurs doivent déclarer tous les facteurs qui pourraient constituer un conflit d'intérêts.

4.4 SUIVI DES ACTIVITÉS DE CERTIFICATION

Le certificateur doit tenir à jour un registre de certification exact, qui indique clairement les progrès liés aux travaux d'évaluation et de certification, et qui fait référence aux décisions prises pendant la certification. Le registre devrait être suffisamment détaillé pour en permettre la traçabilité, en vue d'améliorer la qualité et l'uniformité de l'ensemble de

certifications. Le superviseur peut examiner le registre de certification pour vérifier la traçabilité et assurer l'uniformité par rapport à d'autres certifications.

4.5 CONTRÔLE TECHNIQUE DES ÉVALUATIONS

Le contrôle technique des évaluations est un aspect fondamental de la qualité du programme canadien. Le certificateur effectue trois types d'activités de contrôle :

1. l'examen des preuves d'évaluation produites par l'évaluateur, y compris le rapport technique d'évaluation;
2. la réalisation indépendante d'un sous-ensemble des travaux d'évaluation;
3. l'observation directe des activités d'évaluation choisies (présence aux tests).

4.6 CONTINUITÉ DE L'ASSURANCE

Le Centre pour la cybersécurité suit l'approche définie par les Critères communs pour la continuité de l'assurance avec ses évaluations, un processus dans le cadre duquel l'organisme de certification évalue les changements apportés aux produits déjà certifiés afin de déterminer si le produit peut faire l'objet d'un sous-ensemble de tests plutôt que d'une réévaluation complète. Le Centre pour la cybersécurité évalue la nature des changements apportés au produit de TI en examinant le rapport d'analyse d'impact du développeur et détermine si les changements sont suffisamment mineurs pour que le maintien de l'assurance soit une option appropriée.

4.7 DÉLIVRANCE DES CERTIFICATS LIÉS AUX CRITÈRES COMMUNS, DES RAPPORTS DE CERTIFICATION ET DES RAPPORTS DE MAINTENANCE

Le Centre pour la cybersécurité produit un certificat et un rapport de certification connexe pour chaque évaluation de produit réussie et les affiche sur le portail international des Critères communs (en anglais seulement). Dans le cas de la continuité de l'assurance, le Centre pour la cybersécurité produit un rapport de maintenance et l'affiche comme addenda à l'entrée correspondante du produit certifié sur le portail des Critères communs.

4.8 RÉSOLUTION DES PROBLÈMES TECHNIQUES

Le Centre pour la cybersécurité s'engage à résoudre rapidement les problèmes techniques qui pourraient survenir au cours d'une évaluation. Le Centre pour la cybersécurité distribuera une version épurée du problème ainsi qu'une solution à tous les laboratoires de test, si le problème est important pour tous les laboratoires de test. Les directives s'appliqueront ensuite à toutes les évaluations subséquentes.

4.9 ÉCHANGE D'INFORMATION AVEC LES INTERVENANTS

Le Centre pour la cybersécurité communique avec les intervenants au besoin. Plus précisément, le Centre pour la cybersécurité organise des réunions en personne avec les intervenants des laboratoires de test pour discuter des questions d'intérêt pour l'ensemble du programme et des changements à venir qui ont une incidence sur le fonctionnement du programme.

4.10 ÉCHANGE D'INFORMATION

Le Centre pour la cybersécurité utilise le protocole TLP (en anglais seulement) pour échanger de l'information avec des entités qui ne font pas partie du gouvernement du Canada. Plus précisément, le Centre pour la cybersécurité désigne l'information comme suit :

- l'information sur le programme public porte la mention TLP:WHITE;
- l'information sur les programmes non publics porte la mention TLP:GREEN;
- l'information exclusive ou commerciale confidentielle porte la mention TLP:AMBER.

4.11 GESTION DE LA DOCUMENTATION

Dans le contexte du programme lié aux Critères communs, la documentation comprend tout document qui fournit des preuves objectives d'activités ou de résultats du programme. Il peut s'agir autant d'un document papier que d'un document électronique (y compris les courriels). Voici des exemples de documents :

- documents administratifs ou axés sur la qualité de l'organisme de certification;
- documents de certification des laboratoires de test;
- documents de certification des produits;
- documents de certification des profils de protection;
- documents sur la continuité de l'assurance.

Le Centre pour la cybersécurité tient à jour les documents liés aux Critères communs par voie électronique dans le système ministériel de gestion de l'information du CST.

Le Centre pour la cybersécurité utilise des systèmes ministériels de gestion des TI et des documents qui respectent les politiques du gouvernement du Canada en matière de traitement de l'information, de sécurité et de ressources humaines. Ces politiques font en sorte que le Centre pour la cybersécurité conserve les documents pendant la période minimale de cinq ans exigée par l'ARCC.

4.12 CONFIDENTIALITÉ ET INTÉGRITÉ DES RENSEIGNEMENTS LIÉS AUX CRITÈRES COMMUNS

Le Centre pour la cybersécurité traite les renseignements de nature délicate obtenus dans le cadre des activités liées aux Critères communs selon les normes du gouvernement du Canada pour le traitement des renseignements des niveaux PROTÉGÉ.

Le Centre pour la cybersécurité stocke les dossiers et les documents liés aux Critères communs dans son système ministériel de gestion de l'information. Ce système fournit des enregistrements de vérification sur tous les accès et sur toutes les modifications de ces enregistrements, ainsi qu'un historique des versions qui permet de récupérer les versions antérieures des documents, s'il y a lieu.

En outre, le Centre pour la cybersécurité réserve l'accès aux documents de programme de nature délicate aux membres du personnel de l'organisme de certification.

4.13 DOCUMENTATION DU PROGRAMME

Le Centre pour la cybersécurité tient à jour les versions officielles de la documentation du programme dans ses systèmes ministériels de gestion de l'information. Le Centre pour la cybersécurité tient à jour des copies des versions actuelles de la documentation publique de l'organisme de certification sur le site Web du Centre pour la cybersécurité, notamment :

- les guides (p. ex. le présent document), qui fournissent de l'information sur les services offerts par l'organisme de certification;
- les *Instructions du Programme canadien lié aux Critères communs*, qui fournissent de l'information sur les politiques du Centre pour la cybersécurité sur divers sujets.

Le Centre pour la cybersécurité utilise également des procédures fonctionnelles privées internes et des modèles de documents pour fournir au personnel de l'organisme de certification des descriptions détaillées d'une vaste gamme de fonctions et de responsabilités.

Le Centre pour la cybersécurité utilise les versions officiellement approuvées des *Critères communs pour l'évaluation de la sécurité des technologies de l'information* (en anglais seulement) et de la *Méthodologie commune pour l'évaluation de la sécurité des technologies de l'information (CME)* (en anglais seulement). Le Centre pour la cybersécurité veille à ce que tous les intervenants du programme aient accès à ces documents.

4.13.1 APPROBATIONS DES MISES À JOUR DE LA DOCUMENTATION

Toutes les mises à jour de la documentation du programme lié aux Critères communs doivent être approuvées par la direction du Centre pour la cybersécurité avant d'être publiées. Ces approbations doivent être stockées à un endroit approprié dans le système ministériel de gestion de l'information du Centre pour la cybersécurité. Voici la liste des pouvoirs d'approbation des documents en fonction du rôle le plus élevé dont il est question dans la documentation :

Rôle le plus important pour la documentation	Pouvoir d'approbation
Certificateur ou certificateur principal	Superviseur des Critères communs
Superviseur des Critères communs	Gestionnaire, Assurance et normes des produits
Gestionnaire, Assurance et normes des produits	Directeur, Programmes d'atténuation des risques
Directeur ou Programmes d'atténuation des risques	Directeur général, Partenariats et atténuation des risques

La haute direction du Centre pour la cybersécurité peut, à sa discrétion, exiger des pouvoirs d'approbation plus élevés pour les approbations que ceux énumérés dans ce tableau. Les autorités d'approbation peuvent également subdéléguer leurs pouvoirs dans la mesure où cette délégation se fait par écrit et que le Centre pour la cybersécurité enregistre une copie de la délégation dans le système ministériel de gestion de l'information du Centre pour la cybersécurité.

4.13.2 GESTION DU CHANGEMENT

Le Centre pour la cybersécurité examine chaque année l'ensemble du système de gestion de la qualité. S'il y a lieu, le Centre pour la cybersécurité fournit aux laboratoires de test des versions provisoires des documents mis à jour afin qu'ils puissent

les examiner et donner une rétroaction avant leur dernière mise au point. Le Centre pour la cybersécurité informe par courriel les intervenants directs du programme de tous les changements apportés au programme et publie des mises à jour à l'intention de toutes les parties intéressées dans la section des nouvelles du site Web du programme (https://cyber.gc.ca/fr/programme-canadien-des-criteres-communs).

Afin d'éviter toute confusion entre les versions des documents, le Centre pour la cybersécurité retire tous les documents remplacés de son site Web, de sorte que seules les versions actuellement en vigueur, ou celles qui sont sur le point d'entrer en vigueur, sont accessibles au public.

5 PLAINTES, DIFFÉRENDS ET APPELS

Le personnel du Centre pour la cybersécurité a l'obligation de faire tous les efforts raisonnables pour résoudre les désaccords avec les parties externes de manière à ce que les parties n'aient pas besoin de porter plainte ou de faire appel de façon officielle. Toutefois, lorsque les parties ne peuvent régler un désaccord de façon informelle, le Centre pour la cybersécurité informe la partie externe de son droit de présenter une plainte officielle ou d'exprimer un différend par écrit. En l'occurrence, les plaignants doivent donner suffisamment de détails pour permettre une évaluation adéquate. Si le plaignant n'est pas satisfait du règlement de sa plainte ou de son différend, il peut faire appel.

Le Centre pour la cybersécurité s'engage à traiter rapidement et efficacement toutes les plaintes et tous les différends internes et externes, et il fournira au demandeur une estimation du temps qu'il faudra pour arriver à un règlement. Les tentatives de règlement des plaintes et des différends devraient être d'abord adressées au superviseur du programme lié aux Critères communs; cependant, les appelants peuvent soumettre la plainte à l'un des fonctionnaires énumérés à la section 3.1.

Les plaignants doivent envoyer leurs plaintes et leurs différends par courriel au Centre de services à la clientèle du Centre pour la cybersécurité. Le Centre pour la cybersécurité fournit aux plaignants les coordonnées des personnes-ressources, lorsqu'un appel est nécessaire ultérieurement.

Le Centre pour la cybersécurité utilise les définitions suivantes pour les déclarations écrites :

- **Plainte :** mécontentement à l'égard d'un service fourni par le Centre pour la cybersécurité ou l'un des laboratoires de test.
- **Différend :** désaccord avec une décision prise par le Centre pour la cybersécurité.
- **Appel :** mécontentement à l'égard du règlement d'une plainte ou d'un différend.

5.1 RÔLES ET RESPONSABILITÉS

Le gestionnaire, Assurance et normes des produits, est responsable de ce qui suit :

- Répondre aux appels découlant de plaintes ou de différends présentés précédemment;
- Veiller à ce que la haute direction du Centre pour la cybersécurité soit au courant des appels qui pourraient lui être adressés.

Le superviseur du programme lié aux Critères communs est responsable de ce qui suit :

- Enregistrer la plainte, le différend ou l'appel dans le Système de gestion de la qualité;
- Résoudre la plainte ou arbitrer le différend au nom du Centre pour la cybersécurité;
- Fournir les détails de la résolution à toutes les parties concernées;
- S'assurer que le gestionnaire, Assurance et normes des produits, est au courant de toute plainte ou de tout différend reçu par le Centre pour la cybersécurité.

Les certificateurs principaux et les certificateurs ont les responsabilités suivantes :

- Informer le superviseur de tout désaccord avec les laboratoires de test qui pourrait donner lieu à une plainte officielle ou à un différend.

5.2 PLAIGNANTS

Les plaintes, les différends et les appels formulés par les laboratoires de test doivent provenir des directeurs de laboratoire. De même, ceux qui émanent des commanditaires de l'évaluation doivent provenir d'un cadre supérieur. Le Centre pour la cybersécurité traitera les plaintes, les différends et les appels des autres parties au cas par cas.

5.3 PROCESSUS DE TRAITEMENT DES PLAINTES OU DES DIFFÉRENDS

À la réception de la plainte ou du différend, le superviseur examine les documents pertinents pour la plainte ou la décision contestée et discute du problème avec les certificateurs concernés ainsi qu'avec les certificateurs principaux. Dans le cas d'une plainte, le superviseur fait enquête sur les circonstances qui ont mené à la plainte et peut en discuter. Pour les différends, le superviseur examine le fondement de la décision contestée. Dans les deux cas, le superviseur prend une décision, documente les détails du règlement (y compris la justification connexe), l'enregistre dans le système de gestion de la qualité, informe le plaignant par écrit du règlement (en indiquant son droit d'appel, le cas échéant), et précise le délai dans lequel le plaignant peut faire appel de la décision.

Au moment du règlement de la plainte ou du différend, le superviseur examine le règlement pour déterminer les répercussions sur les politiques ou les procédures de l'organisme de certification et mettra celles-ci à jour, s'il y a lieu.

5.4 PROCESSUS D'APPEL

Comme il est expliqué précédemment, les parties peuvent faire appel des décisions rendues par écrit (relativement aux différends ou aux plaintes) auprès du superviseur ou de l'un des fonctionnaires énumérés à la section 3.1, en faisant parvenir une copie au superviseur. Les parties doivent faire appel dans les cinq jours ouvrables suivant la notification de la décision par le Centre pour la cybersécurité.

Lorsqu'il reçoit l'appel, le superviseur en accuse réception, l'enregistre dans le système de gestion de la qualité et l'envoie au gestionnaire, Assurance et normes des produits, pour que celui-ci prenne des mesures.

Le gestionnaire, Assurance et normes des produits, examine l'appel, la décision contestée et la justification de la décision contestée avec le superviseur. Le gestionnaire décide ensuite d'accepter l'appel et de réviser la décision contestée ou de rejeter l'appel. Le gestionnaire informe ensuite l'auteur de l'appel de sa décision. Lorsque le gestionnaire a refusé l'appel, il informe le plaignant de son droit de faire appel auprès de la haute direction du Centre pour la cybersécurité en lui fournissant les coordonnées appropriées pour cette marche à suivre. Le gestionnaire informe la haute direction du Centre pour la cybersécurité des résultats de l'appel et de la possibilité d'un recours hiérarchique.

Dans les cas où le gestionnaire infirme une décision contestée, le superviseur évalue l'incidence sur d'autres décisions, sur toutes les politiques et procédures du Programme canadien lié aux Critères communs et sur toute activité commerciale au niveau de l'ARCC international. Le superviseur informe toutes les autres parties en cause dans l'appel (p. ex. laboratoires de

test, commanditaires de l'évaluation) de la décision d'appel et de ses répercussions, et met à jour toute la documentation connexe.

6 UTILISATION DES CERTIFICATS, DES MARQUES ET DES LOGOS DE CERTIFICATION

Le Centre pour la cybersécurité fournit des certificats liés aux Critères communs, des marques de commerce connexes et des logos pour indiquer officiellement qu'un laboratoire de test a évalué une version donnée d'un produit de TI conformément aux exigences du Programme canadien lié aux Critères communs.

6.1 UTILISATION ABUSIVE DES CERTIFICATS

Le Centre pour la cybersécurité enquêtera rapidement suivant tout signalement de l'utilisation abusive d'un certificat, d'une marque de commerce ou d'un logo liés aux Critères communs provenant du programme canadien et demandera au titulaire de certificat de prendre rapidement les mesures correctives qu'il juge nécessaires. Si un titulaire de certification ne se conforme pas rapidement, le Centre pour la cybersécurité peut retirer le certificat ou prendre d'autres mesures correctives.

Lorsqu'un laboratoire de test termine avec succès une évaluation, en plus du certificat du produit, le superviseur envoie également une lettre au commanditaire de l'évaluation qui précise les conditions suivantes :

- Les titulaires de certificat peuvent associer le certificat lié aux Critères communs et la marque de certification liée aux Critères communs seulement à la version exacte du produit évalué. Il est interdit au titulaire du certificat d'associer le certificat lié aux Critères communs ou la marque de certification liée aux Critères communs à une version non évaluée du produit.
- Les titulaires de certificat ne doivent pas utiliser le certificat lié aux Critères communs ni la marque de certification liée aux Critères communs d'une manière qui pourrait discréditer le Centre pour la cybersécurité, le Programme canadien lié aux Critères communs ou l'ARCC.
- Les titulaires de certificat doivent aviser le Centre pour la cybersécurité de toute modification apportée au produit certifié et de toute plainte reçue concernant la conformité du produit aux Critères communs.
- Le certificat lié aux Critères communs et la marque de certification liée aux Critères communs demeurent la propriété du CST, et ce dernier peut révoquer la permission de les utiliser à sa seule discrétion. Le CST prendra les mesures appropriées pour prévenir l'utilisation abusive du certificat lié aux Critères communs ou de la marque de certification liée aux Critères communs.
- L'autorisation d'utiliser le certificat lié aux Critères communs et la marque de certification liée aux Critères communs ne constitue pas ni ne sous-entend, directement ou indirectement, l'approbation du produit par le CST.

Le Centre pour la cybersécurité enquêtera sur toute situation où 1) un produit certifié ne peut plus répondre aux critères de certification ou 2) un fournisseur ne respecte pas les conditions de certification. Le Centre pour la cybersécurité peut retirer un certificat s'il le juge nécessaire dans de telles circonstances et avisera le titulaire du certificat par écrit avant de mettre à jour la liste des produits certifiés et le Portail des Critères communs.

7 CONTENU COMPLÉMENTAIRE

7.1 LISTE D'ABRÉVIATIONS, D'ACRONYMES ET DE SIGLES

Terme	Définition
ARCC	Arrangement de reconnaissance des Critères communs
CCN	Conseil canadien des normes
CEM	Méthodologie d'évaluation commune (*Common Evaluation Methodology*)
CST	Centre de la sécurité des télécommunications
TI	Technologies de l'information
TLP	Traffic Light Protocol