Choose a building block.

Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

Canadian Common Criteria Program

Quality Manual

FOR COMMON CRITERIA PRACTITIONERS

Canada

FOREWORD

This document *Canadian Common Criteria Program Quality Manual* is an UNCLASSIFIED publication. It supersedes *Canadian Common Criteria Scheme: Quality Manual Guide #2, version 3.1, October 2016*.

EFFECTIVE DATE

This publication takes effect on March 1, 2020.

REVISION HISTORY

Revision	Amendments	Date
1.0	Initial public release	August 2004
2.0	Major update reflecting a revised structure for Common Criteria program Guides, Instructions and Functional Procedures	September 2010
3.0	Modification of the processes for evaluation eligibility and evaluation acceptance.	August 2016
3.1	Merging of the sections describing the approaches for document management and records management. Updated the section on Periodic Review of Operations.	October 2016
4.0	Significant overhaul to better align the document with CCRA requirements and Cyber Centre publication practices.	March 2020

OVERVIEW

This document is the quality manual for the Canadian Common Criteria program run by the Canadian Centre for Cyber Security. This document describes the organization and policies of the program to meet the international obligations of the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ANNEXES

1 INTRODUCTION

This document outlines the operation of the Canadian Common Criteria program. The Common Criteria is an information technology (IT) testing program based on the international standard ISO/IEC 15408 [1][1] where licensed testing laboratories can evaluate the cyber security of IT products. Consumers of IT products can increase their confidence in the security provided by these IT products via Common Criteria product evaluations.

The Canadian Centre for Cyber Security (CCCS, hereafter the Cyber Centre), a branch of the Communications Security Establishment (CSE), runs the Canadian Common Criteria program and performs the role of certification body, overseeing evaluations performed by commercial IT security evaluation facilities (hereafter testing labs) to ensure quality.

The Communications Security Establishment (CSE), on behalf of the Government of Canada, is a signatory to the international *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security* (CCRA) [2], which provides a framework for international mutual recognition of Common Criteria evaluation results among participating countries.

Other CCRA signatory countries recognize Canadian Common Criteria product certificates. This process of mutual recognition allows a vendor to evaluate their IT product with a testing lab in the country of their choice, rather than contracting multiple redundant evaluations in several countries.

1.1 AUDIENCE

The primary audience for this document is the staff of the certification body, as they have direct responsibility for ensuring quality within the Canadian program. Secondary audiences include testing labs and evaluation sponsors (vendors), as they have a direct interest in the success of certifications and may benefit from an understanding of the certification body's procedures to ensure quality. Other audiences of this document may include consumers of IT security products, as well as other international CCRA signatories.

1.2 POLICY DRIVERS

This document meets the requirements for Certification Bodies from the CCRA [2].

1.3 OUTLINE OF THIS DOCUMENT

This document continues as follows:

- Section 2 describes the certification body
- Section 3 describes the organization of the certification body and its personnel
- Section 4 describes the activities of the certification body
- Section 5 describes how the certification body resolves disputes with participants

[1] Numbers in square brackets indicate reference material. There is a list of references in the Supporting Content section of this document.

- Section 6 describes how the certification body protects the Common Criteria mark

2 CERTIFICATION BODY

2.1 OVERVIEW

The Cyber Centre staffs the certification body. All certification body staff are employees of the Government of Canada and are subject to Government of Canada policies, rules, and regulations, including those that deal with the protection of sensitive information and conflict of interest situations. Per its role as the certification body, the Cyber Centre performs several functions, including:

- Approving testing labs to operate under the Canadian program
- Qualifying evaluators within the testing labs
- Performing technical oversight of evaluations
- Issuing and withdrawing Common Criteria certificates
- Producing certification reports
- Producing assurance maintenance reports
- Maintaining a Certified Products List for evaluations that have completed under the Canadian program
- Representing Canada as a signatory to the CCRA.

2.2 LEGAL STATUS AND AUTHORITIES

The Cyber Centre is a branch of the Communications Security Establishment (CSE), a department of the Government of Canada authorized under the CSE Act [3] as the national technical authority for cyber security and information assurance. The Canadian government provides the funding to operate the Common Criteria program as part of the Cyber Centre's responsibility to provide services to help protect the electronic information and information infrastructures of Canadian federal institutions as well as those designated as being of importance by CSE's minister.

2.3 CONTACTING THE CERTIFICATION BODY

The Cyber Centre operates the Canadian Common Criteria program, and the principal point of contact for external inquiries is the supervisor of the Common Criteria program. Readers may contact the program as follows:

Mail	Email
Common Criteria c/o Canadian Centre for Cyber Security P.O. Box 9703, Terminal Ottawa, Ontario K1G 3Z4 Canada	contact@cyber.gc.ca

2.4 QUALITY MAINTENANCE POLICY

The Cyber Centre is committed to ensuring that its staff conduct all the certification body activities to the standards required by the CCRA. The Cyber Centre expects all staff to perform their duties with integrity, impartiality, and objectivity by following the policies and procedures documented in the quality management system.

The Cyber Centre conducts regular corporate reviews to assess the effectiveness of the quality management system and identify areas for improvement for the certification body's operations and procedures.

2.5 CERTIFICATION FEES

The Cyber Centre ensures its services are available without undue financial conditions by not charging for its Common Criteria certification services.

2.6 NON-DISCRIMINATION POLICY

The Cyber Centre provides non-discriminatory operation and administration of the certification body's services and functions and will not impose undue financial or other conditions on any applicant.

2.7 IMPARTIALITY, VALUES AND ETHICS

All certification body staff shall perform their assigned duties in an impartial, objective, and fair manner. As CSE employees, all certification body staff are subject to the CSE Ethics Charter [4], which includes conflict of interest guidelines that address CCRA requirement C.2.

2.8 PERIODIC REVIEW OF OPERATIONS

The Cyber Centre conducts periodic reviews of all certification body operations. These reviews assess the effectiveness and relevance of certification body policies and procedures, whether the certification body continues to meet the needs of the Government of Canada, and whether the certification body continues to share the objectives of the CCRA.

3 CERTIFICATION BODY PERSONNEL

3.1 ORGANIZATION

The Canadian Common Criteria program consists of the following roles:

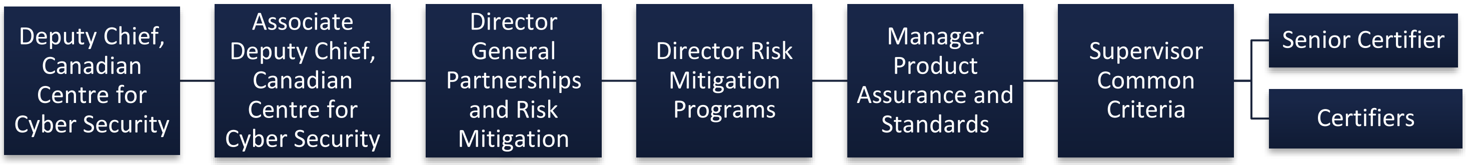
Deputy Chief, Canadian Centre for Cyber Security
Associate Deputy Chief, Canadian Centre for Cyber Security
Director General Partnerships and Risk Mitigation
Director Risk Mitigation Programs
Manager Product Assurance and Standards
Supervisor Common Criteria
Senior Certifier
Certifiers

Figure 1 Certification body organization chart

3.2 ROLES AND RESPONSIBILITIES

To ensure that staff perform their duties in an efficient and effective manner, this document defines the responsibilities and minimum education, experience, and relevant knowledge for all certification body staff.

3.2.1 ALL CERTIFICATION BODY STAFF

All certification body staff members must follow the directions provided in certification body documentation. Staff shall ensure that the supervisor of the Common Criteria is aware of any deficiencies or errors in any of the quality management system documentation.

3.2.2 DIRECTOR RISK MIGITATION PROGRAMS

The director of Risk Mitigation Programs is the head of the certification body and the executive responsible for Canada's participation in the international CCRA program. The organization diagram in section 3.1 shows the reporting structure of the director of Risk Mitigations Programs to the senior executives of the Canadian Centre for Cyber Security. The director is responsible for:

- Approving the strategic direction of the program
- Approving program operations and activities

3.2.3 MANAGER PRODUCT ASSURANCE AND STANDARDS

The manager of Product Assurance and Standards is the certificate-issuing authority for the program and is responsible for effective and efficient operations. In particular:

- Communicating strategic direction to the program's supervisor
- Overseeing the program management activities of the program supervisor
- Ensuring the evolution of the quality management system
- Representing Canada on occasion on the international CCRA Management Committee

- Handling complaints, disputes, and appeals within the certification body

This role requires extensive IT and IT security knowledge gained through a combination of formal education and relevant experience.

3.2.4 SUPERVISOR COMMON CRITERIA

The supervisor of the Common Criteria (hereafter the supervisor) fulfils the role of operations manager and quality manager for the program. The supervisor is responsible for:

- Fulfilling the role of operational manager and quality manager for the program
- Acting as the primary liaison for both technical and non-technical issues
- Providing both technical and administrative direction to staff
  - Ensuring that certification body staff understand their roles and responsibilities
  - Defining the requirements for technical oversight of evaluations
  - Ensuring that the document for evaluation and certification methods is correct and current
- Managing the day-to-day certification operations of the program
  - Accepting new evaluations into the program
  - Assigning certification teams for evaluations
  - Approving certification reports
- Monitoring the performance and operation of the quality management system
  - Reporting issues upward in the management chain
  - Conducting periodic reviews
  - Implementing changes resulting from internal or external review
  - Tracking and monitoring all reports of non-conformities
  - Ensuring that corrective action and preventative measures occur as appropriate
- Overseeing testing lab
  - Validating the knowledge and experience credentials for evaluator candidates, to assess their eligibility to write the Evaluator Exam
  - Grading the Evaluator Exam
  - Assigning qualified technical assessors to assist the Standards Council of Canada (SCC) in the accreditation of testing labs
- Reviewing, on a periodic basis, the effectiveness of existing policies, guidelines, and procedures, and developing new or revised approaches as required
- Acting as first point of contact for complaints, disputes, and appeals, and tracking these until completion
- Representing the program on international CCRA committees, such as the Development Board, Executive Subcommittee and Management Committee.

This role requires:

- A university degree or college diploma in either computer science, computer/electrical engineering, or mathematics, or equivalent knowledge gained through relevant work experience
- Comprehensive knowledge of theories and principles of IT security, computer security evaluation, and certification methods
- Extensive experience with the Common Criteria and Common Methodology for Information Technology Security Evaluation (CEM) [5], gained by direct involvement with its development and/or application
- Experience dealing with vendors, consultants, and international organizations/partners

3.2.5 CERTIFIER

The certifier is primarily responsible for:

- Declaring any conflicts of interest related to their evaluations to the supervisor
- Performing technical oversight of evaluations conducted by testing labs
    - Ensuring the technical quality of the results and conformance to the Common Criteria, CEM, or Protection Profiles
    - Assessing the quality of evaluation activities
    - Observing evaluation activities performed by the testing lab
    - Assessing documentation providing by the testing lab
    - Providing technical direction to testing labs to resolve problems
- Performing technical oversight of assurance maintenance requests
- Producing certification reports and maintenance reports
- Assisting senior certifiers with the tasks necessary to approve new testing labs
- Providing technical oversight and assistance during the SCC re-assessment of testing labs

This role requires:

- University degree or college diploma in either computer science, computer/electrical engineering, or mathematics, or equivalent knowledge gained through relevant work experience
- Knowledge of the theories and principles of IT security, computer security evaluation, and certification methods

3.2.6 SENIOR CERTIFIER

The senior certifier is responsible for:

- All activities of a Certifier
- Ensuring that the technical methods of the program are correct and consistent
- Producing interpretations of the Common Criteria, CEM, and Protection Profiles

- Advising the supervisor on all technical aspects of the program including the effectiveness of policies, guidelines, and procedures
- Providing advice and guidance to certifiers about the management of certifications, and the application and interpretation of the Common Criteria, CEM, and Protection Profile
- Performing the tasks necessary for approval of new testing labs
  - Providing training sessions for candidate evaluators
  - Developing and administering Common Criteria Evaluator Exams to candidate evaluators
- Participating in international CCRA committees

This role requires:

- University degree or college diploma in either computer science, computer/electrical engineering, or mathematics, or equivalent knowledge gained through relevant work experience
- Comprehensive knowledge of the theories and principles of IT security, computer security evaluation, and certification methods
- Significant experience in the Common Criteria and CEM, gained by direct involvement with its development and/or application

3.3 TRAINING REQUIREMENTS

The Cyber Centre follows Government of Canada recruitment and staffing procedures when filling vacant positions within the certification body to ensure the hiring of the most suitable staff members for the certification body. The Cyber Centre considers any certification body staff members who do not meet the minimum qualifications as detailed in the earlier sections as in training. The supervisor closely supervises and monitors the performance of all trainees.

The Cyber Centre maintains information on the relevant qualifications, training, and experience of all certification body staff within its corporate enterprise resource planning and information management systems as per the Government of Canada's processes for human resources management [6].

The Cyber Centre recognizes that certifiers can gain skills and knowledge through a combination of structured training courses, programs of self-study, and supervised on-the-job-training. Certification body staff shall have a personalized training plan to ensure their continued development and will go through annual performance evaluations.

3.4 CONTRACTORS

The certification body does not currently employ any contractors in the performance of tasks. If the Cyber Centre were to use contractors in the future, such contractors would abide by all Canadian program policies and procedures and would receive supervision to ensure adherence to these policies and procedures as well as the quality of their work.

4 CERTIFICATION BODY ACTIVITIES

The following sections briefly describe the activities performed by the Cyber Centre and identify the measures in place to ensure quality.

4.1 APPROVING NEW TESTING LABS

The Cyber Centre must formally approve a testing lab before it may conduct evaluations under the Canadian Common Criteria Program. Please see *Canadian Common Criteria Program: Evaluation Facility Approval* [7] for more information on the approval of testing labs.

The Cyber Centre and each testing lab jointly sign a formal agreement covering all relevant procedures including arrangements for ensuring confidentiality of protected information and the evaluation and certification processes.

4.2 ACCEPTING EVALUATIONS

The Cyber Centre considers products in accordance with *Canadian Common Criteria Program Instructions* [8]. Note that upon acceptance of an evaluation the evaluation sponsor may request a non-disclosure agreement with the Cyber Centre.

4.3 ASSIGNING CERTIFIERS

In assigning a certifier to an evaluation, the supervisor considers several factors, including:

- Depth of knowledge in the Common Criteria, CEM, and applicable Protection Profiles
- Technology-specific knowledge
- Opportunities for certifier training
- Conflict of interest considerations.

In particular, certifiers must not have a vested interest in the success or failure of the certification, in order to comply with Government of Canada ethics guidelines. Accordingly, certifiers must declare any and all factors that might constitute a conflict of interest.

4.4 TRACKING CERTIFICATION ACTIVITIES

The certifier shall maintain an accurate certifier tracking log that clearly identifies progress against evaluation and certification activities, and references decisions made during the course of the certification. The log should contain a level of detail that allows for traceability after the fact for the purposes of quality improvement and consistency across certifications. The supervisor may review the certifier log to verify traceability and ensure consistency with other certifications.

4.5 TECHNICAL OVERSIGHT OF EVALUATIONS

The technical oversight of evaluations is a fundamental aspect of quality in the Canadian program. The certifier performs three types of oversight activities:

1. Examining evaluation evidence produced by the evaluator, including the Evaluation Technical Report
2. Independently performing a subset of the evaluation work
3. Directly observing selected evaluation activities (test witnessing).

4.6 ASSURANCE CONTINUITY

The Cyber Centre follows the defined Common Criteria approach to assurance continuity (*Assurance Continuity: CCRA Requirements* [9]) with its evaluations, a process where the certification body assesses changes made to previously certified products to determine if the product can undergo a subset of testing rather than a full re-evaluation. The Cyber Centre assesses the nature of the changes to the IT product by reviewing the Impact Analysis Report from the developer and determines whether the changes are sufficiently minor that assurance maintenance is an appropriate option.

4.7 ISSUING CC CERTIFICATES, CERTIFICATION REPORTS AND MAINTENANCE REPORTS

The Cyber Centre produces a certificate and associated certification report for each successful product evaluation and posts them to the international Common Criteria portal [10]. In the case of assurance continuity, the Cyber Centre produces a maintenance report and posts it as an addendum to the corresponding certified product entry on the Common Criteria portal.

4.8 RESOLVING TECHNICAL ISSUES

The Cyber Centre commits to promptly resolving technical issues that may arise during an evaluation. The Cyber Centre will circulate a sanitized version of the issue and its resolution to all testing labs if the issue is of importance to all testing labs. This guidance will then apply to all subsequent evaluations.

4.9 SHARING INFORMATION WITH STAKEHOLDERS

The Cyber Centre communicates with stakeholders as issues require it. In particular, the Cyber Centre convenes face-to-face meetings with the testing labs to discuss issues of interest to the whole program, and upcoming changes that affect the operation of the program.

4.10 INFORMATION SHARING

The Cyber Centre uses the Traffic Light Protocol [11] for the sharing of information with parties external to the government of Canada. Specifically, the Cyber Centre marks:

- Public program information with TLP:WHITE;
- Non-public program information with TLP:GREEN; and

- Proprietary or commercial-in-confidence information with TLP:AMBER

4.11 RECORDS MANAGEMENT

A record in the context of the Common Criteria program is a document that provides objective evidence of the activities or results of the program and includes hard copy and electronic documents (including email). Examples of records include:

- Certification body administrative and quality records
- Testing lab certification records
- Product certification records
- Protection Profile certification records
- Assurance Continuity records

The Cyber Centre maintains most Common Criteria records electronically in the CSE corporate information management system. The Cyber Centre stores any required paper copies of documents in a secure filing cabinet on Cyber Centre premises for a period of at least five (5) years before transferring them to the corporate information management team for archival storage in a records office and registry.

The Cyber Centre uses corporate IT and records management systems that follow Government of Canada policies for information handling, security, and human resources. These policies ensure that the Cyber Centre keeps records for the five-year minimum required by the CCRA.

4.12 CONFIDENTIALITY AND INTEGRITY OF COMMON CRITERIA INFORMATION

The Cyber Centre treats sensitive information obtained in the course of Common Criteria activities using the Government of Canada's standards for the handling of PROTECTED information [12]

The Cyber Centre stores all Common Criteria records and documentation in its corporate information management system. This system provides audit records on all access and modification of these records, as well as a version history that allows for the recovery of earlier versions of documents as required.

The Cyber Centre further limits access to sensitive program documents to staff members of the certification body.

4.13 PROGRAM DOCUMENTATION

The Cyber Centre maintains the official versions of program documentation within its corporate information management systems. The Cyber Centre maintains copies of the current versions of the certification body's public documentation on the Cyber Centre website, including:

- Guides (such as this document) that provide information related to the services offered by the certification body
- The *Canadian Common Criteria Program Instructions* [8] that provide information about the Cyber Centre's policies on a variety of topics.

The Cyber Centre also uses internal private functional procedures and document templates to provide certification body staff with detailed descriptions for a wide range of duties and responsibilities.

The Cyber Centre uses the officially endorsed versions of the *Common Criteria for Information Technology Security Evaluation* [1] and the *Common Methodology for Information Technology Security Evaluation (CEM)* [5]. The Cyber Centre ensures that all program stakeholders have access to these documents.

4.13.1 APPROVALS FOR DOCUMENTATION UPDATES

All updates to Common Criteria program documentation requires internal Cyber Centre management approvals prior to release. These approvals shall be stored in an appropriate location within the Cyber Centre's corporate information management system. The following lists the approval authority for documentation based on the most senior role that has authorities discussed within the documentation:

Most Senior Role in Documentation	Approval Authority
Certifier or Senior Certifier	Supervisor of the Common Criteria
Supervisor of the Common Criteria	Manager of Product Assurance and Standards
Manager of Product Assurance and Standards	Director Risk Mitigation Programs
Director or Risk Mitigation Programs	Director General, Partnerships and Risk Mitigation

Cyber Centre senior management may choose at its discretion to require higher levels of authority for approvals than listed in this table. Approval authorities may also sub-delegate their authorities so long as this delegation occurs in writing and that the Cyber Centre store a copy of the delegation within the Cyber Centre corporate information management system.

4.13.2 CHANGE MANAGEMENT

The Cyber Centre reviews the entire quality management system on an annual basis. The Cyber Centre provides, where applicable, draft versions of updated documentation to testing labs for private review and feedback prior to finalization. The Cyber Centre informs direct program stakeholders of all program changes via email and posts updates in the news section of the program's website (https://cyber.gc.ca/en/canadian-common-criteria-program) for all interested parties.

To avoid confusion between document versions, the Cyber Centre removes all superseded documentation from its website so that only the versions currently in effect, or those about to come into effect, are publicly available.

5 COMPLAINTS, DISPUTES AND APPEALS

Cyber Centre staff have an obligation to make every reasonable effort to resolve disagreements with outside parties in such a manner that the parties do not require a formal complaint or appeal. However, when parties cannot resolve a disagreement informally then the Cyber Centre will inform the outside party of their right to submit a formal complaint or dispute in writing. Complainants must submit a complaint or dispute in writing with sufficient detail to permit a proper assessment. If the originator is not satisfied with the resolution of their complaint or dispute, then they may initiate an appeal.

The Cyber Centre commits to dealing with all internal and external complaints and disputes promptly and effectively - and will provide an estimate to the originator for how long it will take to provide a resolution. Attempts to resolve complaints and disputes should start with the supervisor of the Common Criteria program; however, appellants may submit the complaint to any of the officials listed in section 3.1.

Complainants should send complaints and disputes via email to the Cyber Centre's Contact Centre at contact@cyber.gc.ca. The Cyber Centre will provide complainants with contact information if there is a need for a subsequent appeal.

The Cyber Centre uses the following definitions for written statements:

- **Complaint:** A dissatisfaction with a service provided by the Cyber Centre or one of the testing labs.
- **Dispute:** A disagreement with a decision made by the Cyber Centre.
- **Appeal:** A dissatisfaction with the resolution of a complaint or dispute.

5.1 ROLES AND RESPONSIBILITIES

The manager of Product Assurance and Standards is responsible for:

- Responding to appeals arising from previously submitted complaints or disputes
- Ensuring that Cyber Centre senior management is aware of any appeals that may escalate to them.

The supervisor of the Common Criteria program is responsible for:

- Entering the complaint, dispute, or appeal as a record in the Quality Management System
- Resolving the complaint or arbitrating the dispute on behalf of the Cyber Centre
- Providing details of the resolution to all affected parties.
- Ensuring that the manager of Product Assurance and Standards is aware of any complaints or disputes received by the Cyber Centre.

Senior certifiers and certifiers are responsible for:

- Informing the supervisor informed of any disagreements with the testing labs that have the potential to result in a formal complaint or dispute.

5.2 COMPLAINANTS

Complaints, disputes, and appears from testing labs must come from Lab directors. Likewise, those coming from evaluation sponsors must come from a senior manager. The Cyber Centre will handle complaints, disputes, and appeals from other parties on a case-by-case basis.

5.3 COMPLAINT OR DISPUTE PROCESS

Upon receipt of the complaint or dispute, the supervisor reviews the relevant records for the complaint or disputed decision and discusses the issue with the certifiers involved as well as the senior certifier(s). In the case of a complaint, the supervisor investigates the circumstances that led to the complaint and may discuss. For disputes, the supervisor reviews the basis for the contested decision. In both circumstances, the supervisor takes a decision, documents the details of the resolution (including associated rationale), enters it as a record in the quality management system, notifies the complainant in writing of the resolution (informing them of their right to appeal as appropriate), and specifies a timeframe within which they may appeal the decision.

Upon resolution of the complaint or dispute, the supervisor will review the resolution for any impact on certification body policies or procedures and update them as appropriate.

5.4 APPEAL PROCESS

Parties may submit written appeals of decisions made with respect to disputes or complaints as described above to the supervisor or to any of the officials listed in section 3.1, copying the supervisor. Parties must submit appeals within 5 working days of the Cyber Centre's notification of the decision.

Upon receiving the appeal, the supervisor acknowledges receipt, enters it as a record in the quality management system, and forwards it to the manager of Product Assurance and Standards for action.

The manager of Product Assurance and Standards reviews the appeal, the contested decision, and the rationale for the contested decision with the supervisor. The manager then decides whether to accept the appeal and revise the contested decision or decline the appeal. The manager then informs the originator of the outcome. If the manager declined the appeal, the manager will inform the complainant of their right to appeal to Cyber Centre senior management, providing appropriate contact information for that course of action. The manager will inform Cyber Centre senior management of the results of the appeal and of the possibility for an escalation.

In cases where the manager overturns a contested decision, the supervisor will assess the impact on other decisions, on all Canadian CC Program policies and procedures, and on any business activities at the international CCRA level. The supervisor will inform any other involved parties in the appeal (e.g., testing labs, evaluation sponsors) of the appeal decision and its impact, and will update any related documentation.

6 USE OF CERTIFICATES, CERTIFICATION MARKS AND LOGOS

The Cyber Centre provides Common Criteria certificates, related trademarks, and logos to officially indicate that a testing lab evaluated a particular version of an IT product to the requirements of the Canadian Common Criteria Program.

6.1 MISUSE OF CERTIFICATES

The Cyber Centre will promptly investigate any reported misuse of a Common Criteria certificate, trademark or logo originating from the Canadian program and will seek prompt corrective action from a certificate holder as it considers necessary. If a certification holder does not comply promptly, the Cyber Centre may withdraw the certificate or pursue further corrective action.

When a testing lab successfully completes an evaluation, in addition to the product certificate the supervisor also issues a letter to the evaluation sponsor that specifies the following conditions:

- Certificate holders may associate the Common Criteria certificate and the Common Criteria certification mark only with the exact version of the evaluated product. Certificate holder are forbidden from associating either the Common Criteria certificate or the Common Criteria certification mark with any unevaluated product versions
- Certificate holders shall not use either the Common Criteria certificate or the Common Criteria certification mark in a manner that might discredit the Cyber Centre, the Canadian Common Criteria program, or the CCRA
- Certificate holders must advise Cyber Centre of any changes made to the certified product, and all complaints received relating to the product's compliance with the Common Criteria
- The Common Criteria certificate and Common Criteria certification mark remain the property of the Communications Security Establishment and the Cyber Centre may revoke permission to use them at its sole discretion. The Communications Security Establishment will take appropriate action against misuse of the Common Criteria certificate and/or the Common Criteria certification mark
- Permission to use the Common Criteria certificate and the Common Criteria certification mark does not constitute or imply, directly or indirectly, product endorsement by the Communications Security Establishment

The Cyber Centre will investigate any situations where (1) a certified product may no longer meet the certification criteria or (2) a vendor violates certification conditions. The Cyber Centre may withdraw a certificate as it deems necessary under such circumstances and will notify the certificate holder in writing before updating the Certified Products list and the Common Criteria portal.

7 SUPPORTING CONTENT

7.1 LIST OF ABBREVIATIONS

Term	Definition
CCCS	Canadian Centre for Cyber Security
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology
CSE	Communications Security Establishment
IT	Information Technology
SCC	Standards Council of Canada
TLP	Traffic Light Protocol

7.2 REFERENCES

Number	Reference
1	Common Criteria for Information Technology Security Evaluation. Available from https://www.commoncriteriaportal.org/cc/
2	Arrangement on the Recognition of Common Criteria Certificates. Available from https://www.commoncriteriaportal.org/ccra/
3	Communications Security Establishment Act. https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/third-reading#enH3105
4	Communications Security Establishment. Ethics Charter. Available from https://cse-cst.gc.ca/en/about-apropos/ethics-
5	Common Criteria. *Common Methodology for Information Security Technology Evaluation*. Available from https://www.commoncriteriaportal.org/cc/
6	Treasury Board of Canada Secretariat. *Policy Framework for People Management*, 15 July 2010. Available from https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=19134
7	Canadian Common Criteria Program: Evaluation Facility Approval.
8	Communications Security Establishment. Canadian Common Criteria Program Instructions. Available from https://cyber.gc.ca/
9	Common Criteria. *Assurance Continuity: CCRA Requirements*. Available from https://www.commoncriteriaportal.org/files/operatingprocedures/2012-06-01.pdf
10	Common Criteria Portal. Available from https://commoncriteriaportal.org.
11	FIRST. *Traffic Light Protocol (TLP)*. Available from https://www.first.org/tlp/.
12	Treasury Board of Canada Secretariat. *Directive on Security Management*, 1 July 2019. Available from https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611

A.1 Compliance with CCRA Requirements

This section outlines how this quality manual complies with the requirements of the CCRA.

CCRA Requirement		Related Section(s) in this document
B.2	The Role and Principle Characteristics of the CB	a) 4.1 b) 4.2, 4.3, 4.5, 4.6 c) 4.12 d) 4.8, 4.9 e) 4.5 f) 4.5 g) 4.7 h) 4.7 i) https://cyber.gc.ca/en/certified-products j) 2, 3, 4, 5, 6, 7 k) 5 l) 4.13 m) 2.6, 2.7
B.3	Accreditation and Licensing of Evaluation Facilities	4.1
C.1	General Requirements	2.5, 2.6
C.2	Administrative Structure	2.7, 3.1
C.3	Operational Structure	a) 3.1 b) 2.2 c) 2.1 d) 2.2
C.4	Certification/Validation Personnel	3.3, 3.2, 3.4
C.5	Documentation and Change Control	a) 4.13 b) 4.13.1 c) 4.13.2 d) 4.13.2 e) 4.13
C.6	Records	4.11
C.7	Certification/Validation Procedures	4
C.8	Requirements of Evaluation Facilities	4.1
C.9	Quality Manual	a) 2.4 b) 2.2 c) 3.1, 3.2 d) 3.3 e) 3.1 f) 4.5 g) 6.1 h) 3.4 i) 5
C.10	Confidentiality	4.12
C.11	Publications	https://cyber.gc.ca/en/certified-products 1, 2.1
C.12	Appeals of Conciliation	5
C.13	Management Review	2.8
C.14	Misuse of Common Criteria Certificates	6.1
C.15	Withdrawal of Common Criteria Certificates	6.1