Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

# Canadian Common Criteria Program Requirements and Procedures for Testing Laboratories

**FOR TESTING LABS**

TLP:WHITE





Canada

# FOREWORD

This document *Canadian Common Criteria Program Requirements and Procedures for Testing Laboratories* is an UNCLASSIFIED publication. It supersedes *Canadian Common Criteria Scheme Guide #3: Evaluation Facility Approval, version 3.0, August 2016*.

# EFFECTIVE DATE

This publication takes effect on April 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 | Update to the skills matrix in the Annex, added the section on “Signing the Agreement” | August 2016 |
| 4.0 | Reformatting to the document template for the Canadian Centre for Cyber Security, updates describing some process changes. | April 2020 |

# OVERVIEW

The purpose of this document is to describe the requirements and process by which a commercial organization (hereafter referred to as the company) may become an approved Common Criteria evaluation facility (hereafter a testing lab) operating within the Canadian Common Criteria program.

The primary audience for this document is companies looking for information on becoming a testing lab within the Canadian program. Evaluation sponsors (typically vendors), developers, and consumers may also find information in this document helpful to understand the requirements on testing labs operating within the Canadian program.

# TABLE OF CONTENTS



# LIST OF ANNEXES

# 1 INTRODUCTION

In the Canadian Common Criteria program, commercial organizations operate Common Criteria evaluation laboratories (hereafter testing labs) to perform security evaluations of information technology (IT) products.

This document describes the requirements and procedures for testing labs operating within the Canadian program. This includes the process that a commercial organization (hereafter referred to as the company) may follow to become an approved testing lab.

## 1.1 ABOUT THE CANADIAN COMMON CRITERIA PROGRAM

The Canadian Centre for Cyber Security (hereafter the Cyber Centre) operates the Canadian Common Criteria program and acts as its certification body. The Cyber Centre is the Canadian signatory to the *Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security* [1], more commonly referred to as the Common Criteria Recognition Agreement (hereafter the CCRA). For more information about the operation of the Canadian program, please consult the *Canadian Common Criteria Program Quality Manual* [2].

**NOTE:** A testing lab within the Canadian program may also be called by the CCRA name (licensed laboratories) or the formal name of the Standards Council of Canada (SCC) accreditation (an Information Technology Security Evaluation and Testing (ITSET) facility).

# 2 REQUIREMENTS FOR TESTING LABS

This section discusses requirements that the company must meet to be an approved testing lab.

## 2.1 ITSET FACILITY ACCREDITATION

These requirements ensure that testing labs operate in conformance with ISO/IEC 17025 *General requirements for the competence of testing and calibration laboratories* [3].

**2.1.1.** The company shall have a valid Information Technology Security Evaluation and Testing *(*ITSET) Facility accreditation from the Standards Council of Canada [4].

The Standards Council of Canada and the Cyber Centre will conduct a detailed review of a company's ability to meet all the requirements of ISO/IEC 17025 as part of this accreditation.

## 2.2 CONFLICT OF INTEREST REQUIREMENTS

These requirements ensure that the company will perform all evaluation work without undue influence from within or outside the company.

**2.2.1.** The company shall have procedures in place to ensure that company management does not exert undue influence on the outcome of Common Criteria evaluation activities.

**2.2.2.** If the company is controlled by a parent company, the company shall demonstrate that there is enough separation of control and influence so that the parent company cannot:

- Exert undue influence on the outcome of Common Criteria evaluation activities; or
- Inappropriately access proprietary evaluation information.

**2.2.3.** The company shall have appropriate procedures in place to ensure that there is no conflict of interest between personnel performing (1) advice activities to assist an evaluation sponsor in preparing for a Common Criteria evaluation of their IT product and (2) Common Criteria evaluation activities for that product.

**2.2.4.** The company shall inform the Cyber Centre within ten working days after any changes to the ownership or management of the company.

## 2.3 SECURITY REQUIREMENTS

These requirements ensure that the company can safeguard sensitive information.

**2.3.1.** The company shall have a *Designated Organization Screening* as defined in the Public Services and Procurement Canada (PSPC) Industrial Security Manual [5]. All company personnel shall, as a minimum, receive an *Enhanced Reliability Check* from PSPC.

## 2.4 PHYSICAL FACILITY REQUIREMENTS

These requirements ensure that the company operates within the jurisdiction of the Canadian Common Criteria program.

**2.4.1.** The company shall keep a permanent physical facility in Canada with enough office space and equipment available for at least one member of the Cyber Centre to perform evaluation technical oversight as required.

**2.4.2.** The company shall have, or be able to provide with reasonable notice, an IT infrastructure that can support all evaluator functions.

## 2.5 PERSONNEL REQUIREMENTS

These requirements ensure that the company has the qualified personnel to perform a Common Criteria evaluation.

**2.5.1.** The company shall employ at least three staff members who have evaluator certificates issued by the Cyber Centre.

**2.5.2.** At least one staff member shall meet the following requirements for designation as a lead evaluator:

- Must be based in Canada; and
- Must have performed the role of Common Criteria evaluator for a minimum of six months during the previous two years, within a CCRA certificate-authorizing program with which the Cyber Centre has a high degree of familiarity.

**2.5.3.** The company shall inform the Cyber Centre within ten working days following the departure of any qualified Common Criteria evaluators from the testing lab.

## 2.6 TECHNICAL PROFICIENCY

These requirements ensure that the company has the technical competence to perform a Common Criteria evaluation.

**2.6.1.** The company shall perform a successful trial evaluation (see section 3.4) for a Cyber Centre approved IT product, performing evaluation activities in compliance with the requirements of the *Canadian Common Criteria Program Instructions* [6], the *Common Criteria for Information Technology Security Evaluation* [7], the *Common Methodology for Information Security Evaluation* [8], and one or more Protection Profiles [9].

**2.6.2.** The company shall perform all evaluations to the quality standards required from the Cyber Centre.

# 3 PROCEDURES FOR TESTING LABS

## 3.1 BECOMING A TESTING LAB

This section describes the steps that a company will follow to become an accredited testing lab.

1. Ensure that the company can meet the requirements of Section 2.
2. Contact the Cyber Centre via contact@cyber.gc.ca to communicate interest in becoming a testing lab providing the following information:
    a. Full legal name of the company;
    b. Location of the testing lab; and
    c. Coordinates for a primary point of contact.

    The Cyber Centre will confirm whether it is currently accepting new applications for testing labs.
3. Demonstrate all testing lab requirements from Section 2
    a. Contact the Standards Council of Canada to obtain an ISO/IEC 17025 accreditation with an ITSET scope.
    b. Communicate with the Cyber Centre regarding the remainder of the requirements.
4. Enter into a formal agreement with the Cyber Centre to become an accredited testing lab.

## 3.2 MAINTAINING A TESTING LAB

Companies must continue to meet all requirements to keep their status as approved testing labs. Testing labs that do not meet all requirements or to comply with shortcomings identified by the Cyber Centre may result in a company losing the approval to operate a testing lab.

The Cyber Centre may revoke a company's approval to operate a testing lab under the following circumstances:

- The company does not meet the requirements for testing labs and does not correct any deficiencies identified by the Cyber Centre within a reasonable timeframe as specified by the Cyber Centre; or
- The company brings disrepute to the Canadian Common Criteria program, namely through poor performance of evaluations or through non-compliance with the rules of the Canadian Common Criteria program, including, but not limited to, misuse of logos associated with the Canadian Common Criteria program or the CCRA.

## 3.3 QUALIFYING COMMON CRITERIA EVALUATORS

The Cyber Centre requires that all evaluators possess evaluator certificates. Candidates need to demonstrate the following to obtain an evaluator certificate:

1. Demonstrate a score of 9 or more on the evaluator skills matrix (see Annex A); and
2. Achieve a score of 66% on the evaluator exam.

Evaluator certificates do not transfer automatically between testing labs if evaluators change companies. In cases where a candidate previously held an evaluator certificate, the Cyber Centre may choose to recognize this previous qualification, considering the candidate's evaluation history and the length of time that has elapsed since the candidate's most recent Common Criteria evaluation.

To obtain evaluator certificates, a company must provide the Cyber Centre with a current resumé and a completed evaluator skills matrix (see Annex A) for each candidate. The Cyber Centre will validate the evaluator skills matrix and offer successful candidates the opportunity to write the evaluator exam. This exam tests an evaluator candidate's understanding of the Common Criteria, Common Evaluation Methodology and current Protection Profiles.

The Cyber Centre expects that evaluator candidates will have strong working knowledge of the subject matter prior to writing the Evaluator Exam. The Cyber Centre offers a half-day workshop immediately before every exam that focuses on the structure and requirements of the Common Criteria and Common Evaluation Methodology, highlights some current Protection Profiles, and provides specific details on requirements and practices specific to the Canadian Common Criteria Program.

Candidates will obtain evaluator certificates based on their exam results. Candidates with a grade of 66% or higher obtain evaluator certificates. Candidates with a grade between 60% and 65% become apprentice evaluators, whereas those with a grade below 60% must attempt the exam again.

Apprentice evaluators can obtain an evaluator certificate by demonstrating the ability to perform Common Criteria evaluations in practice. The testing lab is responsible for creating a learning plan for apprentice evaluators, for review by the Cyber Centre. The company provides periodic updates to the Cyber Centre on the candidate's progress, and the Cyber Centre determines when an apprentice evaluator obtains an evaluator certificate.

## 3.4 PERFORMING TRIAL EVALUATIONS

The purpose of a trial evaluation is to demonstrate that the company can meet requirement 2.6.1. In addition, the trial evaluation provides an opportunity for a staff member to meet the lead evaluator requirement (requirement 2.5.2). The trial evaluation also completes the Proficiency Testing part of the ITSET accreditation (requirement 2.1.1).

For the trial evaluation, the company evaluates an IT product deemed suitable by the Cyber Centre. The IT product must meet the eligibility requirements of the Canadian Common Criteria Program Instructions [6] and the Cyber Centre will verify that the IT product has a sufficient scope of security functionality to allow the company to demonstrate its evaluation capability. The company manages all commercial arrangements with the evaluation sponsor for this trial evaluation.

During the trial evaluation, the Cyber Centre will examine some evaluation activities in greater depth than for normal Common Criteria evaluations. The Cyber Centre will evaluate the company's ability to:

- Perform evaluation activities in compliance with the *Canadian Common Criteria Program Instructions* [6], the *Common Criteria for Information Technology Security Evaluation* [7], the *Common Methodology for Information Security Evaluation* [8], and Protection Profiles [9] as applicable.;
- Produce evaluation evidence (including Observation Reports) during the evaluation;
- Respond to Observation Reports raised by the Cyber Centre;
- Produce an Evaluation Technical Report documenting the findings; and
- Work as a coordinated team to successfully perform the evaluation.

If the Cyber Centre assesses that the company successfully completed a high-quality evaluation, then the Cyber Centre will post the trial evaluation to the Certified Products List on the international Common Criteria Portal. The Cyber Centre will balance the assessment of the company's performance on the trial evaluation against the realization that the trial evaluation will likely be a learning experience for the company.

Should the trial evaluation not be completed due to issues with either the IT product's ability to meet Common Criteria requirements or the evaluation sponsor, the Cyber Centre may require that the company perform another trial evaluation. This will depend on the extent that the Cyber Centre successfully observed and interacted with the company across a range of evaluation activities.

Unsatisfactory performance will result in the company not receiving Cyber Centre approval to become a testing lab.

# 4 SUPPORTING CONTENT

## 4.1 LIST OF ABBREVIATIONS

| Term | Definition |
|---|---|
| CCRA | Arrangement on the Recognition of Common Criteria Certificates |
| ISO/IEC | International Organization for Standardization / International Electrotechnical Commission |
| IT | Information Technology |
| ITSET | Information Technology Security Evaluation and Testing |
| PSPC | Public Services and Procurement Canada |
| SCC | Standards Council of Canada |

## 4.2 REFERENCES


| Number | Reference |
|---|---|
| [1] | Common Criteria. *Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security*. Available from https://www.commoncriteriaportal.org/files/CCRA%20-%20July%202,%202014%20-%20Ratified%20September%208%202014.pdf . |
| [2] | Communications Security Establishment. *Canadian Common Criteria Program Quality Manual*. Available from https://cyber.gc.ca/en/guidance/quality-manual-guide-2 . |
| [3] | ISO/IEC 17025: *General requirements for the competence of testing and calibration laboratories* |
| [4] | Standards Council of Canada. *Requirements and Guidance for the Accreditation of Information Testing Technology Security Evaluation and Testing Facilities*. Available from https://www.scc.ca/en/about-scc/publications/criteria-and-procedures/scc-requirements-and-guidance-for-accreditation-information-technology-security-evaluation-and |
| [5] | Public Services and Procurement Canada (PSPC). *Industrial Security Manual*. Available from https://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/index-eng.html |
| [6] | Communications Security Establishment. *Canadian Common Criteria Program Instructions*. Available from https://cyber.gc.ca/en/guidance/canadian-common-criteria-program-instructions. |
| [7] | Common Criteria. *Common Criteria for Information Technology Security Evaluation*. Available from https://commoncriteriaportal.org/cc/. |
| [8] | Common Criteria. *Common Methodology for Information Technology Security Evaluation*. Available from https://commoncriteriaportal.org/cc/. |
| [9] | Common Criteria. *Protection Profiles*. Available from https://www.commoncriteriaportal.org/pps/ . |

# Annex A Evaluator Skills Matrix

Cyber Centre evaluators will use this annex as the following assessment tool to evaluate a candidate based on their resume.

| Description | Description | Score |
|---|---|---|
| Familiar | • Has read basic concepts of subject | 0 |
| Working | • Worked on at least one project of at least 4 months effort and demonstrated skills to a supervisor.<br>• This experience can include significant time spent on a project in an academic environment | 1 |
| Comprehensive | • Applied skills/knowledge for at least 2 years in a non-academic environment.<br>• Experience gained while completing a master's degree/Ph.D. may be considered on a case-by-case basis. | 2 |
| Expert | • Recognized in Industry as an Expert in that field.<br>• Published/collaborated on subject matter books, taught courses | 3 |

**NOTES:**

- The Cyber Centre does not consider skills or experience as a supervisor or manager relevant to the work performed as an evaluator. Details should be directly related to experience in a technical, non-supervisory role.
- Candidates should estimate the actual time spent on an activity when estimating the duration of work experience for each category.

# A.1 Candidate Information

| | |
|---|---|
| **Date** | |
| **Candidate Name** | |
| **Testing Lab** | |

# A.2 Formal Education

| Category | Description | Score |
|---|---|---|
| Degree or Certificate | | |
| **Total score for Formal Education (maximum of 3 points)** | | |

**NOTE:** Select the category that gives the most points from the following cases:

- College Certificate: 1 point for an applicable technology or technical certificate
- Bachelor's degree: 2 points for a bachelor's degree from an accredited university, in computer science, electrical engineering or applicable science-related field.
- Graduate degree: 3 points for a master's degree or Ph.D. from an accredited university, in computer science, electrical engineering or applicable science-related field.).

# A.3 Testing Experience

| Category | Description | Duration | Score |
|---|---|---|---|
| **System Testing:** Includes testing at the network level, and interoperability testing of different interconnected IT products. | | | |
| **IT Product Testing:** Feature verification, and debugging | | | |
| **Compliance Testing:** Testing IT products against defined standards. | | | |
| **Vulnerability Testing:** Testing products or networks for security vulnerabilities. | | | |
| **Courses:** e.g., automated test tools, practical software testing techniques | | | |
| **Total score for Testing Experience (maximum of 4 points)** | | | |

## A.4 IT Security Knowledge

| Category | Description | Duration | Score |
|---|---|---|---|
| **IT Security Policy and Procedures:** writing, developing, and implementing | | | |
| **Threat-Risk-Assessments:** Conducting and writing TRAs, safeguard selection | | | |
| **Network Security:** IDS, VPN, Firewalls, etc. | | | |
| **Communications Security:** wireless, cell phones, etc. | | | |
| **Cryptography:** algorithms, protocols, FIPS 140 | | | |
| **IT Security Standards:** writing, implementing, incorporating | | | |
| **Professional Qualifications:** (e.g., CISSP) | | | |
| **IT Security Courses:** (describe each of the courses) | | | |
| **Total score for IT Security Knowledge (maximum of 5 points)** | | | |

## A.5 Product Development

| Category | Description | Duration | Score |
|---|---|---|---|
| **Design:** writing functional and detailed design specifications | | | |
| **Programming:** coding components, modules, modifying features | | | |
| **Version/release Control:** using versioning/release tools, implementing procedures | | | |
| **Courses:** (e.g., programming languages, software development techniques) | | | |
| **Total score for Product Development (maximum of 3 points)** | | | |

## A.6 Overall Score

| | |
|---|---|
| **Total Candidate Score (maximum of 15 points)** | |