Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

Canadian Common Criteria Program

Instructions

FOR COMMON CRITERIA PRACTITIONERS

TLP:WHITE

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

Foreword

The *Canadian Common Criteria Program Instructions* is an UNCLASSIFIED publication intended for testing labs operating in the Canadian program. This document supersedes all previous instructions for the Canadian Common Criteria Program, from either the Canadian Centre for Cyber Security or the Communications Security Establishment.

Effective Date

This publication takes effect on June 15, 2022.

Revision History

Revision	Amendments	Date
1.0	First revision of a harmonized set of program instructions. - Incorporated all scheme instructions into a single document. - Reformatted the document using a Canadian Centre for Cyber Security template - Updated content of instructions to reflect process changes	September 30, 2019
1.1	Revision of section on cryptographic functionality.	June 11, 2021
1.2	Added sections for “Core and Essential Functionality”, “Remote Testing” and “Assessing and Addressing Vulnerabilities”	October 25, 2021
1.3	Revised the section on “Evaluation Eligibility”, added a reference document for approved cryptography, updated interim evaluation milestone requirements to remove approval confirmation from the Cyber Centre, amended Testing milestone date to PiE + **4.5** months, de-coupled remote testing proposal from the eligibility stage, harmonized terminology	December 6, 2021
1.4	Incorporated comments from certification body review	December 31, 2021
1.5	Update to Eligibility Section	January 7, 2022
1.6	Updates based on feedback from the testing labs	February 21, 2022
1.7	Updates based on feedback from the testing labs	March 25, 2022
1.8	Formatting changes	June 8, 2022

Overview

This document contains all instructions related to evaluations within the Canadian Common Criteria program.

Table of Contents

1 Introduction

The *Common Criteria for Information Technology Security Evaluation* (also referred to as the Common Criteria, or CC) is an international standard for specifying security requirements for Information Technology (IT) products. The Canadian Centre for Cyber Security (hereafter the Cyber Centre) operates the national Certification Body (CB) for Common Criteria evaluations performed in Canada.

This document includes detailed topics for Common Criteria Testing Laboratories (hereafter testing labs) related to the evaluations performed within the Canadian program. For general information about the Canadian Common Criteria program, please visit the Cyber Centre's Common Criteria website.

2 Evaluation Eligibility

The Cyber Centre accepts evaluations into the Common Criteria program in the following order of priority:

1. Evaluations to Common Criteria Protection Profiles, including:
   - International *collaborative protection profiles* developed by the international technical community; and
   - Selected Protection Profiles and PP-Modules developed by one of the member countries to the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, also referred to as the *Common Criteria Recognition Arrangement*, or CCRA.
2. For technology types where there are no suitable Protection Profiles, other evaluations that fall within the scope of the CCRA; at the time of writing this includes evaluations up to Evaluation Assurance Level (EAL) 2.

The Cyber Centre will also consider accepting evaluations beyond the scope of the CCRA on a case-by-case basis. This includes EAL 3 or EAL 4 evaluations.

3 Core and Essential Functionality

For Evaluation Assurance Level (EAL)-conformant evaluations, where the specification of Security Functional Requirements (SFRs) has not been pre-determined by a Protection Profile, it is important to ensure that the evaluation covers a meaningful set of security functionality. This includes both *Core Functionality* and *Essential Functionality*, as described below.

3.1 Core Functionality

Core functionality is defined as the primary purpose of a product, what a consumer would expect to be included within the scope of the evaluation, and how it is marketed. This may require the creation of extended SFRs in cases where the core functionality of the Target of Evaluation (TOE) cannot be represented by existing SFRs. Any included core functionality should be related to cybersecurity in some manner (vs. functionality that has nothing to do with cybersecurity).

3.2 Essential Functionality

Essential functionality can be defined as functionality that has been deemed important to the cybersecurity of the product (based on the nature of the TOE) by the Cyber Centre, such as Secure Management and Inter-TOE communication.

3.3 Specification of Requirements

Evaluations are required to include the Core Functionality of the TOE and any included Essential Functionality (or lack thereof), and the onus is on the testing lab to provide a rationale for any perceived deficiencies.

4 Timelines for Evaluations

The Cyber Centre recognizes that consumers require security assurance for current versions of IT products, so evaluations need to occur in a timely manner. Modern product lifecycles can be short and the amount of time that a product remains "in evaluation" needs to reflect this.

The Cyber Centre believes that advanced preparation for evaluations - such as a functional gap analysis and preliminary functional testing prior to evaluation – are a necessary part of modern evaluations. As such, the Cyber Centre introduces evaluation milestones and timelines that testing labs must meet for evaluations.

4.1 Evaluation Milestones

The Cyber Centre recognizes the following milestones within evaluations:

1. Security Target;
2. Design/Entropy;
3. Testing; and
4. Final Evaluation.

4.1.1 Security Target Milestone

The Security Target milestone requires that the testing lab complete all evaluation activities associated with the *Security Target Evaluation* assurance class (see section 12 of [1]).

Once the Security Target milestone is complete, the Cyber Centre lists the product on the program's Products in Evaluation list. The date that this happens is the *Product in Evaluation (PiE) Date* for the product.

4.1.2 Design/Entropy Milestone

The Design/Entropy milestone requires that the testing lab complete all evaluation activities associated with the *Development* assurance class (see section 13 of [1]) and where required to meet the claimed Protection Profile (PP), an entropy analysis.

4.1.3 Testing Milestone

The Testing milestone requires that the testing lab complete all required functional and penetration testing.

4.1.4 Final Evaluation Milestone

The Final Evaluation milestone requires that the testing lab successfully complete all evaluation activities.

4.2 Milestone Deadlines

The Cyber Centre applies the following deadlines to the evaluation milestones described in Section 4.1:

Milestone	Deadline
Design/Entropy	PiE Date + 2 months
Testing	PiE Date + 4.5 months
Final Evaluation	PiE Date + 6 months

In order to ensure that the Cyber Centre has adequate time to review the Final Evaluation deliverable, it must be received no later than 2 weeks prior to the milestone deadline.

4.3 Requesting Extensions to Milestone Deadlines

The Cyber Center will consider requests from testing labs for milestone deadline extensions. The testing lab shall detail why they are unable to meet the deadline, propose a reasonable extension period, and describe the measures they will take to meet the new date.

4.4 Missing Milestone Deadlines

When an evaluation misses either of the Design/Entropy or Testing milestone deadlines, the Cyber Centre will remove the IT product from the Products in Evaluation list. However, the testing lab may continue with the evaluation, and the evaluation will remain eligible for certification, provided that the testing lab meets the Final Evaluation milestone deadline.

When an evaluation does not meet the Final Evaluation milestone deadline, then the Cyber Centre will withdraw the evaluation from eligibility for certification. Testing labs will need to reapply for eligibility.

5 Evaluation of Cryptographic Functionality

The Cyber Centre leverages the results of the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) to ensure that evaluators adequately evaluate cryptographic modules and algorithms within the scope of an evaluation.

Note: The Cyber Centre jointly manages the CMVP and CAVP in partnership with the United States National Institute of Standards and Technology (NIST).

5.1 Cryptographic Functionality

- For PP-conformant evaluations, a CAVP certificate is required for the cryptography claimed.
- For EAL-conformant evaluations where the primary purpose of the TOE is cryptography, a CMVP certificate is required for the cryptography claimed.
- For EAL-conformant evaluations where the environment provides cryptography in support of TOE functionality, a CAVP certificate is required for the cryptography claimed.
- For EAL-conformant evaluations where cryptography is used for supporting functionality, a CAVP certificate can be used for the cryptography claimed. Under certain conditions, testing using a Known-Good implementation may be acceptable in lieu of CAVP.

In all cases, only Cyber Centre approved cryptography is to be used. The following publication identifies and describes approved cryptographic algorithms and appropriate methods of use: https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111.

5.2 Verification of Cryptographic Implementations

The Cyber Centre requires that evaluators verify the presence of all cryptographic implementations claimed by the vendor. It is not sufficient for testing labs to merely point to a CAVP/CMVP certificate. This verification can take various forms depending on the type of implementation and the level of access the evaluator has to the underlying functions of the TOE.

5.3 Entropy Assessment

The Cyber Centre requires an entropy assessment whenever there is a conformance claim to a protection profile that includes random number generation (RNG) requirements performed by the TOE. These protection profiles clearly state the cases where the Security Target must claim the RNG functions.

There is no need for an entropy assessment if the Security Target does not include RNG requirements in the scope of the evaluation.

6 Remote Testing

Testing labs are expected to perform testing of products at their facility. In exceptional circumstances, this might not be feasible. What follows are the conditions and requirements of when testing labs may conduct remote testing of products.

6.1 Conditions

Under exceptional circumstances, testing labs may request to test remotely under the following situations:

- If the costs involved in testing/shipping/setup the TOE are prohibitive;
- If the TOE setup/environment is overly complex and requires significant support from the developer;
- If the testing requires specialized tools/equipment that the vendor possesses but cannot provide to the testing lab; or
- Other conditions subject to Cyber Centre approval.

6.2 Requirements

In order to gain approval from the Cyber Centre for remote testing, the testing lab must provide the following details:

- A detailed justification:
  - If claiming cost, provide a high-level breakdown of the costs involved.
  - If claiming complexity, provide a rationale as to why the TOE setup/environment is overly complex.
  - If claiming specialized tools, provide details about the tools and why the testing lab cannot procure them.
- An explanation as to how the evaluator will meet the requirements for AGD_PRE.
- How testing will be performed by the evaluator.
- How control of the test environment will be maintained by the evaluator.
- How witnessing will be accommodated.

The Cyber Centre has final approval of any remote testing requests.

7 Assessing and Addressing Vulnerabilities

IT products receiving a Common Criteria certificate shall not contain known unmitigated security-relevant vulnerabilities.

7.1 Assessment

All potential vulnerabilities discovered during the public domain search or automated tool-based discovery process shall be assessed by the testing lab using criteria provided by the Cyber Centre. The assessment process shall be sufficiently detailed to determine whether the product and its components are free of security-relevant vulnerabilities.

7.2 Addressing

Any actual vulnerabilities identified in the evaluated product shall be addressed. If a vendor patch addressing the vulnerability exists, it needs to be applied. If a vendor patch does not exist, vulnerabilities may be handled by:

- Removing the affected functionality (**Preferred);**
- Disabling the affected functionality and issuing a public notice advising of the issue; or
- Providing a vendor plan for addressing the vulnerability.

The Cyber Centre has final approval on any approaches taken to address vulnerabilities.

8 Supporting Content

8.1 List of Abbreviations

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
NIST	National Institute of Standards and Technology
OSP	Organizational Security Policy
PiE	Product in Evaluation
PP	Protection Profile
RNG	Random Number Generation
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation

8.2 References

Number	Reference
[1]	Common Criteria. *Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components*. Available from https://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf