ACCREDITATION SERVICES

SCC Requirements and Guidance for the Accreditation of Information Technology Security Evaluation and Testing Facilities

2021-03-19

Standards Council of Canada

Open a world of possibilities.

Canada

Standards Council of Canada
55 Metcalfe Street, Suite 600
Ottawa, ON K1P 6L5

Telephone: + 1 613 238 3222
Fax: + 1 613 569 7808
accreditation@scc.ca
www.scc.ca

Permission to Reproduce

Aussi offert en français sous le titre *Exigences et lignes directrices du CCN relatives à l'accréditation des installations d'évaluation et d'essais de produits de sécurité des technologies de l'information*

Table of Contents

Preface

The document *SCC Requirements and Guidance for the Accreditation of Information Technology Security Evaluation and Testing Facilities replaces CAN-P-1591C - Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities (ITSET) - April 2010*.

CAN-P-1621 - Requirements for the Accreditation of Cryptographic Module and Algorithm Testing Facilities - November 2006 is obsolete and will not be replaced since SCC is not offering this accreditation program.

Introduction

The Canadian Centre for Cyber Security (CCCS), a branch of the Communications Security Establishment, operates the Certification Body (CB) for the Canadian Common Criteria Scheme. The Canadian Common Criteria Scheme is a government-industry partnership, whereby commercial evaluation facilities conduct Common Criteria (CC) evaluations of IT security (ITS) products, and the CCCS is also responsible for approval of CC evaluation facilities (CCEF) and utilizes the ITSET-PSA in determining technical competence; successful evaluation facilities receive the Scope of Accreditation identified in Annex B, which is specific to the CC standard.

Facility accreditation identifies the facility as competent and capable to perform security evaluation and testing of ITS products and systems in accordance with defined standards. SCC in partnership with CCCS (the ITS Competent Authority) offers ISO/IEC 17025 accreditation to ITSET facilities under the ITSET Program Specialty Area (ITSET-PSA).

The purpose of this document is to amplify, where appropriate, generic technical and organizational criteria as stated in ISO/IEC 17025 for SCC accreditation of facilities that could perform ITS evaluation and testing. In their respective ITS Approval Domains, recognized ITS Competent Authorities may recognize the accreditation of those facilities for activities such as, but not limited to, the following activity areas:

- Common Criteria product and system evaluations;
- ITS product review
- Secure electronic commerce application evaluations;
- Biometric device testing;
- Vulnerability and tiger team testing; and
- Specialized commercial security device testing.

SCC accredits laboratories for carrying out objective tests. Objective tests will be controlled by:

- Documentation of tests, including test procedures;

- Validation of the tests;
- Training, qualifications and authorization of staff; and
- Maintenance of equipment and facilities.

And, where appropriate, by:

- Calibration of equipment;
- Use of appropriate reference materials;
- Provision of guidance for interpretation;
- Verification of results;
- Testing of staff for proficiency; and
- Recording of equipment and test performance.

1. References

- ISO/IEC 17025:2017 *General Requirements for the Competence of Testing and Calibration Laboratories*.
- ISO/IEC TR 17026:2015 *Conformity assessment -- Example of a certification scheme for tangible products*
- ISO/IEC 15408-1:2009 *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model*
- ISO/IEC 15408-2:2008 Information technology -- *Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components.*
- ISO/IEC 15408-3:2008 Information technology -- *Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components*
- ISO 18045:2008 Information technology -- *Security techniques -- Methodology for IT security evaluation*
- International Vocabulary of Metrology – Basic and General Concepts and Associated Terms (VIM 3rd edition). JCGM 200:2012 (JCGM 200:2008 with minor corrections)
- ISO/IEC 17000:2004 *Conformity Assessment Vocabulary and General Principles.*
- ISO/IEC Guide 2:2004 *General Terms and Their Definitions Concerning Standardization and Related Activities.*
- SCC Accreditation Program Overview
- NIST Handbook 150, NVLAP, Procedures and General Requirements, National Institute of Standards and Technology/National Voluntary Laboratory Accreditation Program (NIST/NVLAP), Gaithersburg, MD USA
- NIST Handbook 150-20 Checklist, Information Technology Security Testing Common Criteria

2. Definitions

All definitions in ISO/IEC 17025:2017 (e.g. laboratory, testing laboratory, calibration laboratory, calibration, test, calibration method, test method, verification, quality system, quality manual, reference standard, reference material, certified reference material, traceability, proficiency testing, accreditation requirements) and those applicable from ISO/IEC 17000 (e.g. quality assurance, quality control) apply, as well as the following items specific to this document.

Approved Signatories: Persons qualified and authorized to sign test reports, and calibration certificates - prerequisite to delivering a test report or calibration certificate to the customer.

Approval: Determination by an information security authority, that a facility is technically competent in a specific activity area for ITS evaluation and testing the formal authorization enabling the facility to carry out testing within the context of the ITSET.

Architectural Design: The conceptual specification of the structure and the operation of the ITS product.

Evaluation: Analysis and conformance testing conducted against national and international security evaluation criteria (e.g. the Common Criteria). Term is equivalent to SCC notion of "testing."

Information Technology Security Evaluation and Testing (ITSET) Facility: *Within the context of SCC accreditation, a* facility that has been accredited by SCC through the ITSET-PSA to conduct security evaluation and testing of ITS products.

Facility: An organization that conducts security evaluations and tests. When the facility is part of an organization that carries out activities in addition to evaluations and tests, the term "facility" refers only to those parts of that organization that are involved in evaluation.

Facility Accreditation: A formal recognition that a facility has met the ITSET accreditation requirements. Facility accreditation identifies the facility as competent and capable to perform security evaluations and tests of ITS products and systems in accordance with ITSET.

ITS Approval Domain: A specialized IT Security area for which a recognized ITS Competent Authority exists, and for which:

a) Standards exist (or will in the future) to govern specialized ITS evaluation and testing activities;
b) There exists a need for evaluating and testing of ITS products or services;
c) The recognition of individual and organizational competencies to perform specialized security evaluation and testing activities exists;
d) The requirement for control and oversight of a specified range of IT security product evaluation and testing exists;
e) There exists a need for reviewing and approving evaluation and testing results and;
f) Accredited SCC ITSET lab(s) exist(s).

Information Technology Security: All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, or access control.

Key Technical Personnel: Facility personnel with the authority and responsibility to make the important technical evaluation decisions. The “chief”, “lead”, or “team leader” evaluator roles are examples.

On-site Assessment: The on-site examination of a facility to assess its compliance with the conditions and criteria for accreditation under the ITSET.

Product: Any IT security technology that is intended to protect assets and which is the target of security Evaluation and Testing activities. Such technologies may range from stand-alone hardware or software components, through to fully integrated systems, and may include any procedural processes on which these technologies are dependant for secure use in the intended environment.

Proficiency Testing: Demonstration by a facility that it can successfully perform testing and evaluation activities applicable to its Scope of Accreditation. Under ITSET, facilities will be required to demonstrate theoretical and applied competence in the conduct of ITS product evaluations and tests.

Records: Documented evidence and data, intended for future reference, of a specific act, analysis, result, event or other activity, that is related to ITS Evaluation and Testing. Records should be kept in an appropriate form (which may be electronic or otherwise) that is permanent for their required useful life as determined by the Recognized ITS Competent Authority.

Recognized ITS Competent Authority: An organization which exercises leadership, official authority or direct influence over a specified ITS Approval Domain to control, and ensure compliance with, appropriate standards and best practices related to evaluation and testing of products within that domain. This organization is responsible for the approval of accredited ITSET facilities to conduct specialized security evaluation and testing activities in order that approval or certification of results for products applicable to the specific ITS Approval Domain may be granted.

Security Requirements: Specification of functionality or design controls for information technology that, when implemented, provide security.

Technical Review: A process whereby an ITSET facility`s evaluation team gains sufficient knowledge of a product to permit a technical judgement regarding its likelihood of satisfying a particular security requirement.

Testing Tools: The complete set of equipment, including any hardware and software utilities and associated documented procedures, which are used to support Security Product Evaluation and Testing activities. Such equipment should be appropriate for the intended use, and should be managed, operated and maintained in accordance with the manufacturer`s requirements and any other appropriate practices.

Validation: Validation of a test tool or procedure is the process of verifying as far as possible that the test tool will behave properly or that the test procedure will produce results that are consistent with the specifications of the relevant test suites, relevant standards, or previously validated versions of the test tool.

3. Scope of Testing

3.1 ITSET activities range from tests with clearly defined results, such as firewall penetration tests, password strength verification tests and biometric false acceptance rate tests, to activities which may require a great deal of interpretation, such as the implementation robustness of the security functions and features of a software/hardware ITS product.

3.2 ITSET involves the analysis of security features implemented within a software/hardware ITS product which can provide the following security services:

- Confidentiality of information;
- Integrity of information;
- Availability; and
- Accountability.

3.3 Specific security features that can be tested for may include but are not limited to the following:

- Identification and authentication;
- Security audit (audit trail generation and secure storage, analysis of security relevant events);
- Non-repudiation;
- Cryptographic services (cryptographic operations, cryptographic key management);
- Secure transport of information (implementation and enforcement of access control and/or information flow rules/policies);
- Stored data integrity;
- Management of security functions, security relevant data and security management roles;
- Protection of security functions, including non-bypassability and domain separation;
- Resource utilization (fault tolerance, priority of service, resource allocation);
- Fail-safe;
- Self-test; and
- Physical protection (tamper detection/prevention).

3.4 Techniques used to evaluate security features may include but are not limited to the following:

- Known answer tests;
- Vulnerability analysis to ensure that that the customer has considered all potential vulnerabilities within the ITS product under evaluation;

- Software code reviews;
- Detailed analysis of the development environment and associated documentation to determine the effectiveness of the configuration management system applicable to the ITS product under evaluation;
- Detailed examination of delivery documentation to determine if it describes adequately all of the procedures required to maintain the integrity of the ITS product under evaluation;
- Examination and testing of installation, generation and start-up procedures to determine if they are complete and sufficiently detailed to result in a secure configuration of the ITS product under evaluation;
- Detailed analysis of development documentation such as functional specifications, high-level designs, low-level designs to ensure they accurately instantiate all interfaces and security functions inherent of the product under evaluation;
- Detailed analysis of user and administrator guidance documentation to determine that it sufficiently and unambiguously describes how to securely use and administer the product, and ensure consistency with the other documentation supplied for the evaluation;
- Examination and assessment of development security procedures during site visits to determine that they detail sufficiently the security measures for the development environment required to protect the confidentiality and integrity of ITS product design and implementation;
- Assessment of customer developed tests in terms of coverage and depth, independent functional tests, and independent penetration tests;
- Security policy mapping; and
- Security requirements tracing.

3.5 Generic ITS Testing Approach

3.5.1 The Security Testing methodology identifies four major elements in the planning and execution of the ITSET facility's security testing: Test Coverage Analysis; Test Plans; Test Procedures; and Test Results.

3.5.2 Test Coverage Analysis is usually comprised of mappings from security features to the tests that demonstrate the correct behaviour of those security features. Test Coverage can be used to demonstrate that all security features have been tested.

3.5.3 The Test Plan describes the extent to which each security feature will be tested, the approach for testing it as well as the resources, such as equipment, personnel and time necessary to carry out such an approach to testing.

3.5.4 The Test Procedures describe the sequence of actions conformant to the Test Plan necessary to set up the test environment, establish the necessary test prerequisite conditions, perform the testing, and document the expected test results. Test Procedures are recorded in sufficient detail to eliminate ambiguity

during test conduct such that other evaluators can repeat the test procedures in the future, and obtain the same test results.

3.5.5 The Test Results document the actual test results observed during testing. These actual test results are recorded in sufficient detail not only to allow comparison with the expected test results, but also to facilitate comparisons if the tests are repeated in the future. Based on the actual test results, a determination can be made regarding correct security behaviour.

4. Assessment Team

4.1 Composition of the Assessment Team

4.1.1 SCC provides the Lead Assessor for each accreditation or re-assessment, and CCCS provides one or more additional Assessors for the on-site assessment and proficiency testing.

4.2 Preparation for On-Site Assessment

4.2.1 The objective of the on-site assessment is to facilitate the demonstration of conformance of the facility's operations to ISO/IEC 17025.

4.2.2 Prior to the on-site assessment the assessors will review the facility management system documentation and staff resumes. Should the assessors require additional documentation from the facility to support proficiency testing, the facility should be notified in advance of the assessment in order to allow for the submission of the requested documentation.

4.3 Proficiency Testing

See Annex B.

ANNEX A: Application of ISO/IEC 17025:2017 Requirements for ITSET Facilities

Applications are considered an elaboration of the generally stated requirements of ISO/IEC 17025:2017 for which testing and evaluation criteria specifically applicable to ITSET will be used. The ISO/IEC 17025:2017 clause numbers for which the application applies are indicated in the following table.

ISO/IEC 17025:2017 Section No.:	SCC Application Notes for ITSET Facilities
4 General Requirements	
4.1.1 4.1.4	• The facility may, at the discretion of the ITS Competent Authority, develop ITS products; and • The facility may, at the discretion of the ITS Competent Authority, provide consulting services for and participate in the ITS testing of the same product. • Risks to impartiality resulting from activities mentioned above shall be identified, and mitigation strategies developed.
5 Structural Requirements	
5.4	When testing is performed at the customer site or other location outside the facility, all ITSET requirements and guidance pertaining to equipment, accommodation and environment shall apply.
6 Resource Requirements	
6.2.2	• At least one technical staff member shall have management responsibilities and extensive experience in ITS. For Common Criteria evaluation facilities the sufficiency of education and ITS experience of facility staff members will be reviewed and assessed against a pre-defined skills matrix developed by the ITS Competent Authority. • The facility shall have at least three technical staff members with appropriate educational background (a university degree or college diploma in computer science, engineering, or a related discipline, or professional certification), or significant relevant work experience in threat modeling, security architecture analysis, penetration testing, or information security compliance.
6.2.5	The Management system shall document the policies and procedures (training program) governing the routine checks of the competence of all of the staff involved in the conduct and evaluation of tests. In the case where only one member of facility staff is competent to conduct a specific aspect of testing, assessment shall

	at a minimum include a review of documentation and instructions, adherence to procedures and instructions, and documentation of the audit findings.
6.3.1	The facility shall maintain an environment capable of conducting ITS evaluations. This includes facilities for security evaluation and testing, staff training, record keeping, document storage and software/hardware storage.
6.3.4	Processes and procedures shall be in place to maintain a logical separation of different products under evaluation during the product testing phase. This includes maintaining a dedicated test setup and associated components, services, and IT servers for each evaluation. Virtualization and software-defined network segmentation are examples of methods which may achieve this goal.
6.4.1	For their scope of accreditation, the facility shall have appropriate hardware, software, and computer facilities to conduct ITS product evaluations and tests. The facility shall maintain on-site systems adequate to support IT security evaluations in keeping with the tests for which it is seeking accreditation. The facility shall have, or be able to provide with reasonable notice, a sufficient IT infrastructure to support: • Word processing, for the production of reports; • Secure e-mail communication with customers, ITS Competent Authority etc.; • Internet access; and, • Specialized tools as may be required for evaluation work.
6.4.3	For ITSET, “equipment” refers to software and hardware products or other assessment mechanisms used by the facility to support the evaluation and testing of the ITS product. The facility shall maintain on-site systems adequate to support ITS product evaluations and test. The equipment used for tests shall be operated and maintained as follows: • In accordance with the manufacturer’s recommendation; and • As specified in the test method; or • As specified in the detailed requirements specific to the program speciality area.

	Facilities shall have procedures describing the creation of test setups and the configuration of individual IT entities that are part of the test setup. These procedures can take the form of discrete SOPs or can be incorporated into the relevant Test Plan for each evaluation. The facility shall have procedures to ensure proper retention, disposal or return of software and hardware after the completion of the evaluation.
6.4.12	The facility shall maintain all hardware and software used during testing by applying appropriate security patches and performing basic hardening as is appropriate. The intent of this requirement is to ensure that test equipment is adequately secured against malicious attackers.
7 Process Requirements	
7.1.1	The ITSET facility and its customer shall agree in writing what constitutes the test item and the environment in which the test item will be tested, including: the specific test item, the test configuration and the external environment. The ITSET facility and the customer shall agree, in writing, to the following: • The specific test item; • The test configuration; • Location(s) of testing/evaluation; • Whether assistance for preparation of evaluation environment will be provided by the customer, such as shipping special equipment to the facility, installing special operating system and database systems, etc.; • Deliverables to be provided by customer; • Deliverables to be produced by facility; and • Facility approach to testing. Final test reports shall be kept by the facility following the completion of testing for the duration specified by the customer and/or the ITS Competent Authority.
7.4.1	The ITSET facility shall have procedures for: • The handling and integrity of products; • The handling and integrity of testing tools and software; and • The conduct of on-site testing.

7.5.1	The facility shall maintain a functional record-keeping system that is used to track test activities for each security product evaluation. Records of evaluation activities shall be traceable to recognized industry standards and methodologies where applicable. Records shall be easily accessible and contain enough evaluation evidence so that an independent body can determine what evaluation work was actually performed and can concur with the verdict. The ITSET facility shall produce records covering the following activities: • Creation of and changes to evaluation procedures and methodology; • Acceptance/rejection of products submitted for evaluation; • Complete tracking of multiple versions of evaluation evidence and evaluation technical reports; • Complete tracking of evaluation activities including initial analysis, verdicts and any subsequent changes to those verdicts (e.g. based upon modifications of evidence or additional analysis); • Information sufficient to reproduce any testing performed during the evaluation; and • The configuration of all test equipment used during an evaluation along with analysis of that equipment to confirm the suitability of test equipment to perform the desired testing. Facility records shall be maintained, released, and/or destroyed in accordance with the facility's proprietary information policy and contractual agreements with customers.
7.8.1.2	The ITSET facility shall issue test reports of its work which accurately, clearly and unambiguously present the test conditions, test set up, test results and all required information.
7.8.3.1 e)	The test report shall reference standard tests or otherwise provide a description of the tests.
8. Management System Requirements	
8.4.2	The facility shall have an effective back-up system in place to restore evaluation evidence (data and records) in the event of their loss.

ANNEX B: Scope of Accreditation for Common Criteria Evaluation Facilities

Introduction

Facility accreditation identifies a facility as competent and capable to perform security evaluations and tests of Information Technology Security (ITS) products and systems. This annex details the specific evaluation/test methods that such facilities may perform under the ISO/IEC 15408 series of standards (also referred to as the *Common Criteria*, or CC) by utilizing the methodology document ISO/IEC 18045.

This annex also details the skills and competencies required of facility staff, and proficiency testing techniques specific to CCEFs.

Scope of Accreditation

In accordance with the following standards:

- ISO/IEC 15408-1:2009 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model
- ISO/IEC 15408-2:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components.
- ISO/IEC 15408-3:2008 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components
- ISO/IEC 18045:2008 Common Methodology for Information Technology Security Evaluation

The scope of accreditation comprises the following evaluation and testing activities:

- APE: Protection Profile Evaluation;
- ASE: Security Target Evaluation;
- EAL1: Evaluation Assurance Level 1;
- EAL2: Evaluation Assurance Level 2;
- ALC_FLR: Flaw Remediation; and
- CCCS-approved collaborative Protection Profiles.

Required Skills and Competencies

For the accreditation scope detailed above, facility staff shall have a working knowledge of ISO/IEC 15408 series and ISO/IEC 18045, and possess the skill and expertise required to perform the following activities in a manner that is compliant with the requirements of ISO/IEC 15048 and ISO/IEC 18045:

- Evaluate a Protection Profile;
- Evaluate a Security Target;
- Perform a detailed analysis of customer development environment and associated documentation to determine the effectiveness of the customer's configuration management system;
- Perform a detailed examination of customer delivery documentation to determine if it describes adequately all of the procedures required to maintain the integrity of the ITS product under evaluation;
- Examine and test installation, generation and start-up procedures to determine if they are complete and sufficiently detailed to result in a secure configuration of the ITS product under evaluation;
- Perform a detailed analysis of development documentation such as functional specifications, high-level designs, low-level designs to ensure they accurately instantiate all interfaces and security functions inherent of the product under evaluation;
- Perform a detailed analysis of user and administrator guidance documentation to determine that it sufficiently and unambiguously describes how to securely use and administer the product, and ensure consistency with the other documentation supplied for the evaluation;
- Examine and assess development security procedures during site visits to determine that they detail sufficiently the security measures for the development environment required to protect the confidentiality and integrity of ITS product design and implementation;
- Perform a vulnerability analysis to ensure that that the customer has considered all potential vulnerabilities within the ITS product under evaluation;
- Perform an assessment of the customer tests in terms of coverage and depth, conduct independent functional tests, and perform independent penetration tests;
- Perform a review the customer's test plan, test approach, test procedure and test results, and examine their test evidence to demonstrate that security functions perform as specified and that the security functionality has been systematically tested against the functional specification and high-level design;
- Develop functional tests by examining customer design and guidance documentation, examining the customer's test documentation, executing a large sample of the customer's test cases, and creating test cases that augment customer tests;
- Develop penetration tests based on vulnerability analysis, functional specifications, high-level designs, low-level designs and installation guidance; and
- Generate observation, evaluation and test reports in accordance with the requirements of the Canadian Common Criteria Scheme.

Proficiency Testing – Technical Oversight Process

As noted above, the CB is responsible for performing technical oversight of CC evaluation work performed by CCEFs. Through this process of technical oversight, the CB can determine whether the CCEF is performing quality evaluations, or whether corrective action needs to be taken by the CCEF. To meet the requirements of technical oversight in the Canadian Common Criteria Scheme the facility should be capable of the following activities:

- Providing an eligibility submission that clearly describes the IT product to be tested, including the Logical Scope of the security functions and an assessment of the potential applicability of any Protection Profiles relevant to the product type;
- Performing evaluation activities in compliance with the requirements of the CC and CEM, and produce evaluation evidence for the CB during the evaluation conduct stage;
- Responding to Observation Reports raised by the CB;
- Producing an Evaluation Technical Report (ETR) documenting the findings; and
- Working as a coordinated team to successfully perform the evaluation.

The CB may choose to observe some evaluation activities more closely or repeat more evaluation activities than would otherwise be the case in other CC evaluations, in order to ensure that appropriate procedures and analysis are being applied. The results of the technical oversight process described above can be used for proficiency testing purposes.

In addition to the technical oversight process the CB assesses, tests, and approves prospective CC evaluators. In order to participate as CC evaluators, personnel are required to demonstrate evidence of ITS education and relevant past experience, and to pass an exam administered by CB to test knowledge and ability in the application of the CC and the CEM. Once individuals successfully complete both of these requirements, the CB issues an evaluator certificate indicating that the evaluator is qualified to perform work under the Canadian Common Criteria Scheme.

SCC considers the above PT framework as adequate in meeting requirements of clause 7.7.2 in ISO/IEC 17025:2017.