MINISTRY OF INVESTMENT, TRADE AND INDUSTRY
DEPARTMENT OF STANDARDS MALAYSIA

STR 1.10 - SPECIFIC TECHNICAL REQUIREMENTS FOR ACCREDITATION OF INFORMATIONTECHNOLOGY SECURITY EVALUATION AND TESTING: COMMON CRITERIA

Issue 2, 20 June 2023

(Supplementary to MS ISO/IEC 17025)

SKIM AKREDITASI MAKMAL MALAYSIA (SAMM)

LABORATORY ACCREDITATION SCHEME OF MALAYSIA

TABLE OF CONTENTS

Introduction

This document shall be used by Department of Standards Malaysia (JSM) to provide appropriate criteria for the assessment and accreditation of laboratories providing Information Technology (IT) Security Evaluation and Testing services using Common Criteria (CC) and Common Evaluation Methodology (CEM).

This document also provides supplementary requirements for any laboratories interested to apply Common Criteria methodology and standard by elaborating on the requirements of MS ISO/IEC 17025. The clause numbers in this document follow those of MS ISO/IEC 17025. Since not all clauses require interpretation, the numbering may not be continuous.

.

1 Scope

1.1 This document shall be read in conjunction with MS ISO/IEC 17025, Accreditation Policy (AP) documents and relevant requirements published by JSM.

1.2 CC is a set of requirements on functional and assurance of ICT products and systems, which provides a common baseline for security evaluation. CC provides assurance that the process of specification, development, implementation and evaluation of IT security product and systems has been conducted in a rigorous and standardised manner.

1.3 CC evaluation and certification programme in Malaysia is regulated by the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme. MyCC encompasses of two (2) key components:

a) Malaysian Security Evaluation Facility (MySEF) – an entity licensed by the MyCC Scheme and accredited to MS ISO/IEC 17025 by Department of Standards Malaysia for the performance of information security testing, inspection and evaluation using CC and CEM; and

b) MyCC Certification Body (MyCB) – an entity to certify the results of evaluation as defined within the scope of certification and evaluation services performed by licensed MySEF. MyCB is recognised by the Common Criteria Recognition Arrangement (CCRA) as the sole certification body in Malaysia and is being subjected to assessment by CCRA on a prescribed interval.

1.4 CC security evaluation and CEM performed by laboratories including MySEF shall use normative references documents as listed in Clause 2.

1.5 For laboratories that are licensed (MySEF) or intend to be licensed under MyCC Scheme, the version of CC and CEM Standards for evaluation shall be governed by the MyCC Scheme.

1.6 The scope of accreditation for laboratories including MySEF performing CC security evaluation shall include but not limited to the following scope:-

a) Security Evaluation of CC Protection Profiles (PP)

A Protection Profile defines set of security requirements for a category of IT products or systems that meet specific consumer needs. This scope shall assess the competency of MySEF in performing the test as specified in CEM requirements.

Security Evaluation of IT products and systems as Target of Evaluation (TOE)

IT products and systems refer to IT software, firmware and hardware that provide security functionality designed for use or to be incorporated with multiple systems. IT product can be a single product or multiple IT products configured as an IT system or system solution to meet customer needs. This scope assesses MySEF competency in evaluating IT products or systems based on CC assurance classes of Evaluation Assurance Level (EAL) and CEM requirements.

2 Normative references

2.1 This document refers to the following standards and referenced documents. For all references, the latest edition of the document applies: -

i. MS ISO/IEC 17025 - General Requirements for the Competence of Testing and Calibration Laboratories, and

ii. Accreditation Policy Documents, and

iii. CCRA published requirements as follows:

a. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model (CC Part 1)

b. Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements (CC Part 2)

c. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements (CC Part 3)

d. Common Criteria for Information Technology Security Evaluation Part 4: Framework for the specification of evaluation methods and activities (CC Part 4)

e. Common Criteria for Information Technology Security Evaluation Part 5: Pre-defined packages of security requirements (CC Part 5)

f. Common Methodology for Information Technology Security Evaluation (CEM)

OR

iv. ISO published documents as follows:

a. MS ISO/IEC 15408-1 – Information technology -- Security techniques -- Evaluation criteria for IT security Part 1 – Introduction and general model

b. MS ISO/IEC 15408-2 – Information technology -- Security techniques -- Evaluation criteria for IT security Part 2 – Security functional requirements

c. MS ISO/IEC 15408-3 – Information technology -- Security techniques -- Evaluation criteria for IT security Part 3 – Security assurance requirements

d. ISO/IEC 15408-4 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities

e. ISO/IEC 15408-5 - Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements

f. MS ISO/IEC 18045 – Information technology -- Security techniques -- Evaluation criteria for IT security– Methodology for IT security evaluation

v. MyCC Scheme Requirement (MYCC_REQ), CyberSecurity Malaysia, and/or

vi. ISCB Evaluation Facility Manual (ISCB_EFM), CyberSecurity Malaysia, and/or

vii. Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security from CCRA portal.

3 Terms and definitions

The relevant terms and definitions given in all the normative references and the following apply: -

3.1 Evaluation

A process where a PP or TOE is being evaluated against a set of CC requirements using CEM.

3.2 Evaluation Assurance Level (EAL)

Levels of CC predefined assurance scale describing the depth and rigor of an evaluation. These EALs consist of an appropriate combination of assurance components as described in Chapter 8 of CC Part 3 or Clause 3.1.27 of MS ISO/IEC 15048.

3.3 Protection Profile (PP)

Implementation-independent statement of security needs for a TOE type.

3.4 Security Target (ST)

Implementation-dependent statement of security needs for a specific identified TOE.

3.5 Target of Evaluation (TOE)

Set of software, firmware and/or hardware possibly accompanied by guidance.

3.6 Test Tool

Software or hardware that supports one or more test activities

4 General requirements

Same as in MS ISO/IEC 17025.

5 Structural requirements

Same as in MS ISO/IEC 17025.

6 Resource requirements

6.1 General

6.1.1 The laboratory shall have necessary resources to manage and perform its laboratory activities.

6.2 Personnel

The laboratory shall have sufficient personnel having appropriate technical knowledge, competence to carry out the evaluation. Personnel competence for MySEF shall comply with the relevant requirements of the ISCB Evaluation Facility Manual (ISCB_EFM).

Note: ISO/IEC 19896-3 provides guidance for knowledge, skills and effectiveness requirements for ISO/IEC 15408 Evaluators.

a. The evaluator shall possess a tertiary education qualification or any professional certifications or any equivalent experience in at least one of those areas identified in table below before they can conduct security evaluation.

Qualification	Description
Relevant tertiary education	Bachelor, Master or higher degree in at least one of the following: o Software engineering o Computer architecture o Computer science o ICT security o Computer engineering o Microcontroller architecture and programming o System analysis and design and/or related field.
Relevant professional certificates	Information Security, Security Engineering, Cryptography, Common Criteria.

To have at least two (2) years working experience or complete one project in common criteria or related ICT security evaluation covering key fundamental domains.

b. Approved signatory shall comply to the requirements stated in the table above with the additional experience of two (2) evaluation projects. This part of the document must be read in conjunction with

the requirements in Accreditation Policy 4 (AP4) - Policy on the Requirements For Key Personnel of Conformity Assessment Bodies.

6.3 Facilities and environmental conditions

6.3.1 In security evaluation and testing laboratory, environmental conditions refer to the testing environments in which hardware and associated software on which the TOE is being tested.

Other activities (testing and non-testing) shall be effectively separated from the environmental conditions in which the TOE being tested to ensure non-interference on the testing activities that could influence the results.

6.3.2 The environmental conditions to ensure correct testing of the TOE shall be documented.

6.3.3 The environmental conditions and TOE identification including its version shall be monitored, controlled and recorded to ensure validity of the result.

6.3.4 Access control to testing area, network, operating systems, application and information related to the evaluation activities that may affect the outcome of the evaluation shall be appropriately controlled.

6.3.5 The environmental conditions for the evaluation and testing performed at site out of its permanent laboratory control including at the customer, developer or user site shall be recorded.

6.4 Equipment

Same as in MS ISO/IEC 17025.

6.5 Metrological traceability

Same as in MS ISO/IEC 17025.

6.6 Externally provided products and services

Same as in MS ISO/IEC 17025.

7 Process requirements

Same as in MS ISO/IEC 17025.

7.2 Selection, verification and validation of methods

7.2.1 Selection and verification of methods

Selection of Methods

The laboratory shall conduct the evaluation using CC and CEM standards. Other CCRA supporting documents, where relevant, shall also be used.

For CC testing, the security evaluation activities shall be traceable to the underlying CC requirements and work units in CEM, to ensure that test results constitute credible evidence.

7.3 Sampling

Same as in the MS ISO/IEC 17025.

7.4 Handling of test items

7.4.1 The laboratory shall protect the TOE from any modification, unintended use or unauthorised access. Procedure to ensure proper storage, retention, disposal or return of software and hardware after the completion of the evaluation shall be established and maintained.

7.5 Technical records

Same as in MS ISO/IEC 17025.

7.6 Evaluation of measurement uncertainty

Evaluation of measurement uncertainty may not be applicable for common criteria evaluation and testing.

7.7 Ensuring the validity of results

The laboratory shall participate in relevant Proficiency Testing program or Interlaboratory Comparison (ILC) where available.

7.8 Reporting of results

The laboratory shall issue Evaluation Technical Report (ETR) which represent the final output from the evaluation project. The content of ETR shall conform to the requirements of CC, CEM, MS ISO/IEC 17025 and relevant policy documents under SAMM and/or MyCC Scheme. For MySEF, ETR shall be submitted to MyCB for review.

The use of accreditation symbol in ETR shall conform to the requirements stated in AP1- Policy on the Use of Accreditation Symbol and Reference to Accreditation.

7.9 Complaints

Same as in MS ISO/IEC 17025.

7.10 Nonconforming work

Same as in MS ISO/IEC 17025.

7.11 Control of data and information management

Same as in MS ISO/IEC 17025.

8. Management system requirements

8.1 Options (Option A)

Same as in MS ISO/IEC 17025.

8.2 Management system documentation (Option A)

Same as in MS ISO/IEC 17025.

8.3 Control of management system documents (Option A)

Same as in MS ISO/IEC 17025.

8.4 Control of records (Option A)

Same as in MS ISO/IEC 17025.

8.5 Actions to address risks and opportunities (Option A)

Same as in MS ISO/IEC 17025.

8.6 Improvement (Option A)

Same as in MS ISO/IEC 17025.

8.7 Corrective actions (Option A)

Same as in MS ISO/IEC 17025.

8.8 Internal audits (Option A)

Same as in MS ISO/IEC 17025.

8.9 Management reviews (Option A)

Same as in MS ISO/IEC 17025.

Bibliography

i. ISO/IEC 19896-3:2018(en) IT security techniques — Competence requirements for information security testers and evaluators — Part 3: Knowledge, skills and effectiveness requirements for ISO/IEC 15408 evaluators

Acknowledgements

1.	Mr. Pua Hiang (Chairman)	Assessor, Department of Standards Malaysia
2.	Ms. Siti Raikhan Aina Bogal (Secretariat)	Department of Standards Malaysia
3.	Mr. Ibrahim Ismail	Unit Pemodenan Tadbiran dan Perancangan Pengurusan Malaysia (MAMPU)
4.	Ms. Haslinda Mat Akhir	MAMPU
5.	Ms. Siti Fatimah Abidin	Cybersecurity Malaysia
6.	Ms. Hasnida Zainuddin	Cybersecurity Malaysia
7.	Ms. Norhazimah Abdul Malek	Assessor, Department of Standards Malaysia
8.	Mr. Alwyn Goh	MIMOS Berhad
9.	Mr. Ashok Sivaji	MIMOS Berhad
10.	Mr. Chan Weng Siang	TUV AUSTRIA Cybersecurity Lab Sdn Bhd
11.	Mr. Wilson Lim	Cybertronics Lab (Across Vertical)
12.	Mr. Saurabh Sarawat	Cybertronics Lab (Across Vertical)