MOSTI

SKIM AKREDITASI MAKMAL MALAYSIA (SAMM)
LABORATORY ACCREDITATION SCHEME OF MALAYSIA

SPECIFIC TECHNICAL REQUIREMENTS 1.10 (STR 1.10) - SPECIFIC TECHNICAL REQUIREMENTS FOR ACCREDITATION OF INFORMATION TECHNOLOGY SECURITY EVALUATION AND TESTING: COMMON CRITERIA

Issue 1, 2 January 2009
(Supplementary to MS ISO/IEC 17025)

MS ISO/IEC 17025

JABATAN STANDARD MALAYSIA
Department of Standards Malaysia

PREAMBLE

The general requirements for the competence of testing and calibration laboratories are described in MS ISO/IEC 17025. These requirements are designed to apply to all types of testing and calibration objective and therefore need to be interpreted with respect to the type of testing and calibration concerned and the techniques involved.

This document does not re-state all the provisions of MS ISO/IEC 17025 and laboratories are reminded of the need to comply with all of the relevant criteria detailed in MS ISO/IEC 17025. The clause numbering in this document follow those of MS ISO/IEC 17025. Where technical interpretation is not required, the clauses will not be included in this document. This document shall be used by accreditation bodies 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).

Laboratories are also reminded of the need to comply with any relevant statutory or legislative requirements.

PURPOSE

This document is intended to provide supplementary requirements for accreditation of Malaysian Security Evaluation Facilities (MySEF) by providing interpretation to the application of MS ISO/IEC 17025.

AUTHORSHIP

This document has been produced in consultation with STANDARDS MALAYSIA Technical Working Group (TWG) 29 of STANDARDS MALAYSIA Technical Working Group Committees.

ABBREVIATIONS

CC	Common Criteria
CCRA	Common Criteria Recognition Arrangement
CEM	Common Criteria Evaluation Methodology
STANDARDS MALAYSIA	Department of Standards Malaysia
EAL	Evaluation Assurance Level
ICT	Information, Communication and Technology
IT	Information Technology
ITSET	Information Technology Security Evaluation and Testing
MyCB	MyCC Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MySEF	Malaysian Security Evaluation Facilities
NCSP	National Cyber Security Policy
PP	Protection Profile
SAMM	*Skim Akreditasi Makmal Malaysia* (Laboratory Accreditation Scheme of Malaysia)
SC	Specific Criteria
ST	Security Target
STR	Specific Technical Requirements
TOE	Target of Evaluation
TWG	Technical Working Group

PAGE

PREAMBLE 1

PURPOSE 1

AUTHORSHIP 1

ABBREVIATIONS 2

1 SCOPE 5

2 REFERENCES 7

3 TERMS AND DEFINITIONS 8

4 MANAGEMENT REQUIREMENTS 9

4.1 Organisation 9

4.2 Management System 10

4.3 Document control 10

4.4 Review of requests, tenders and contracts 10

4.13 Control of records 11

5 TECHNICAL REQUIREMENTS 11

5.1 Introduction and Scope 11

5.2 Personnel 11

5.3 Accommodation and environmental conditions 14

5.4 Test Methods and Method Validation 15

5.5 Equipment 15

5.6 Measurement traceability 16

5.7 Sampling 16

5.8 Handling of test and calibration items 17

5.9 Assuring the quality of test and calibration results 17

5.10 Reporting the results 18

NOTE: Clause numbers correspond to those in the standard MS ISO/IEC 17025

1. SCOPE

This document shall be read in conjunction with MS ISO/IEC 17025 or relevant Specific Criteria (SC) published by Department of Standards Malaysia (STANDARDS MALAYSIA).

1.1 CC is a set of requirements on functional and assurance of ICT products and systems, which provide 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 standard manner.

1.2 CC evaluation and certification programme in Malaysia is regulated by the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme, which was established under the purview of the National Cyber Security Policy (NCSP). MyCC encompasses of two key components:

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

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

1.3 CC security evaluation and CEM performed by MySEF shall use the following standards:

a) MS ISO/IEC 15408 - Information technology -- Security techniques -- Evaluation criteria for IT security and
b) MS ISO/IEC 18045 - Information technology -- Security techniques --

Methodology for IT security evaluation.

The version of CC and CEM Standards for evaluation shall be governed by the MyCC Scheme.

1.4 The scope of accreditation for MySEF performing CC security evaluation shall confine 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 system that meet specific consumer needs. This scope shall assess the competency of MySEF in performing the test as specified in CEM requirements.

b) **Security Evaluation of IT products and systems (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 assess MySEF competency in evaluating IT products or systems based on CC assurance classes of Evaluation Assurance Level (EAL) and CEM requirements.

2. REFERENCES

i. MS ISO/IEC 17025:2005, General requirements for the competence of testing and calibration laboratories.

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

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

iv. MS ISO/IEC 15408-3 – Information technology -- Security techniques -- Evaluation criteria for IT security Part 3 – Security assurance requirements MS ISO/IEC 18045 – Information technology -- Security techniques -- Evaluation criteria for IT security– Methodology for IT security evaluation

v. Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, V3.1 R1, September 2006 (CC Part 1)

vi. Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, V3.1 R2, September 2007 (CC Part 2)

vii. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, V3.1 R2, September 2007 (CC Part 3)

viii. Common Methodology for Information Technology Security Evaluation V3.1 R2, September 2007 (CEM)

ix. MyCC Scheme Policy (MyCC_P1), v1.1, CyberSecurity Malaysia, 14 February 2008.

x. MyCC Evaluation Facility Manual (MyCC_P3), v1.1, CyberSecurity Malaysia, 30 June 2008.

xi. Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

3. TERMS AND DEFINITIONS

For the purposes of this document, the relevant terms and definitions given in MS ISO/IEC 15408 and MS ISO/IEC 18045 apply.

3.1 Evaluation

A process where a PP or TOE is being evaluated against a set of CC requirements using CEM. The term is consistent with the STANDARDS MALAYSIA notion of testing.

3.2 Evaluation Assurance Level (EAL)

Levels of CC predefined assurance scale describing the depth and rigor of an evaluation. There are 7 hierarchically order of EAL defined in CC for the rating of a TOE's assurance. Higher level of EAL, represents higher level of assurance. These EALs consist of an appropriate combination of assurance components as described in Chapter 8 of CC Part 3.

EAL 1 – Functional tested

EAL 2 – Structurally tested

EAL 3 – Methodically tested

EAL 4 – Methodically designed, tested and reviewed

EAL 5 – Semiformally designed and tested

EAL 6 – Semiformally verified designed and tested

EAL 7 – Formally verified designed and tested

3.3 Protection Profile (PP)

An implementation-independent set of security requirements for a category of TOEs that meets specific customer needs.

3.4 Security Target (ST)

An implementation-dependent set of security requirements for a specific identified TOE to be used as a basis of an evaluation.

3.5 Target of Evaluation (TOE)

Subject of an evaluation; a set of software, firmware and/or hardware, and its associated guidance documents.

4. MANAGEMENT REQUIREMENTS

The numbering format of this section of the document corresponds with the clauses in MS ISO/IEC 17025. MySEF shall be referred to "the laboratory" from this section onwards.

4.1 Organisation

4.1.2 The laboratory shall establish and maintain policies and procedures on impartiality and integrity in the conduct of IT security evaluations where;

a) There are clear segregation of duties between developer of a PP, ST or TOE with the evaluator performing evaluation on the same PP, ST or TOE so that impartiality is assured

b) An evaluator shall not evaluate PP, ST or TOE where he or she was involved in providing consultation services in any part of the development process

4.1.3 The laboratory shall establish and maintain policies and procedures on handling of evaluations off sites or in associated temporary or mobile facilities to ensure protection of proprietary information against disclosure to unauthorized parties. Where an evaluation is being performed using equipment or systems controlled by customer, developer or user, a procedure for handling and controlling the evaluation shall be in place.

4.2 Management systems

A Laboratory Quality Manual shall be established and maintained to document the overall implementation of the management systems. The quality document must also cross refer to SAMM Policies and relevant SC or Specific Technical Requirements (STR) endorsed by STANDARDS MALAYSIA.

Laboratory shall establish and maintain the Information Security policy to ensure an appropriate management of information and assets within the management system.

4.3 Document control

Test method may include test plans, test suites and test cases. This should include relevant inputs, evaluation procedures and test design specification which shall be controlled, reviewed, approved and revised.

Document shall be suitably classified based on laboratory's identified classification levels (i.e Top Secret, Secret, Confidential, Restricted or Public) and shall be managed, transferred, stored and disposed in accordance with the procedure appropriate to their classification.

4.4 Review of requests, tenders and contracts

The laboratory should identify associated risks related to any requests or tenders by customers. Terms and conditions to mitigate the associated risks should be identified and documented in the relevant agreement or contracts.

4.13 Control of records

Records shall be suitably classified based on laboratory's identified classification levels (i.e op Secret, Secret, Confidential, Restricted or Public) and shall be managed, transferred, stored and disposed in accordance with the procedure appropriate to their classification.

Laboratories shall have appropriate controls and procedures in place for the collection, storage, manipulation, reduction and transmission of electronic data and results based on their classification level.

5 TECHNICAL REQUIREMENTS

5.1 Introduction

This section of the document shall be read in conjunction with MS ISO/IEC 17025 and SC published by STANDARDS MALAYSIA.

The purpose of this section of the document is to establish specific technical requirements for accreditation of laboratories involved in Information Technology Security Evaluation and Testing (ITSET) using CC and CEM.

5.2 Personnel

The testing laboratory shall have sufficient personnel having appropriate technical knowledge and proficiency to carry out the evaluation. The signatory(ies) shall be knowledgeable in the scope of work sought or accredited.

a) The evaluator shall possess at least tertiary qualification, professional certifications or equivalent experience in the

following areas in Table 1 with at least one year working experience before they can conduct security evaluation.

Qualification	Description
ICT Degree or	• Bachelor, Masters or PhD in Information and Communication Technology that include at least one but not limited to the following: Software engineering • Microcontroller architecture and programming • System analysis and design • Security
Computer Science Degree or	Bachelor, Masters or PhD in Computer Science that include at least one but not limited to the following: • Software engineering • Computer architecture • Microcontroller architecture and programming • System analysis and design • Security
Electronics Engineering Degree or	Bachelor, Masters or PhD in Electronics Engineering that include at least one but not limited to the following: • Microcontroller architecture and programming

Qualification	Description
	• Digital electronics • Analogue electronics
Certified Information System Security Professional (CISSP) or	Applicable to those with IT or IT related Diploma with at least five years of working experience in Information Security or those with non-IT related degree with at least four years of working experience in Information Security.
System Security Certified Practitioner (SSCP) or	Applicable to those with non-IT related tertiary qualification.
Other professional qualification by certification providers	Specific certification by these providers but not limited to the following: • Software and Network Solutions (**SANS**) Incorporated. • The Computing Technology Industry Association (**CompTIA**) • International Information Systems Security Certification Consortium (**ISC^2**)

b) Approved signatory shall comply to the following requirements in Table 1 with at least one year experience in ITSET or related fields and two years of working experience in CC or posses any

professional Information Security Certification. This part of the document must be read in conjunction with the requirements in STANDARD MALAYSIA SAMM Policy 6 (SP6) – Requirements for SAMM Approved Signatory.

5.3 Accommodation and environment conditions

5.3.1 In ITSET, the word “environment” refers to hardware and associated software on which the TOE being tested is running. The laboratory shall ensure that any interference from other activities in the system does not invalidate the result of the specified test.

Procedure to control handling of evaluation performed in an environment controlled by customer, developer or user shall be in place.

5.3.2 The test environment and the TOE under test shall be appropriately recorded and controlled to ensure correct and complete identification at any time.

5.3.3 The laboratory network used to conduct evaluation activities shall be completely isolated.

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

5.4 Test methods and method validation

5.4 2 Selection of Methods

The laboratory shall conduct the evaluation using CC and CEM standards. Other supplementary documents from CCRA should also used. The version of the standards and other supplementary documents to be used shall comply with the requirements of MyCC Scheme as stated in item 1.3 of this document.

5.4.5 Validation of Methods

For the purpose of achieving product certification through MyCC, laboratories shall require to comply with standards and policies or guidance documents outlined by MyCC Scheme.

5.4.6 Measurement uncertainty

Measurement uncertainty refers to an estimate of the possible error in a measurement. Estimate of the range of values which contain true value of the measured quantity or probability of the true value lies within a stated range of values.

Due to qualitative nature of evaluation in IT security testing, using CC, determination of measurement uncertainty is not applicable

5.5 Equipment

Within the scope of ITSET, equipment used for evaluation shall include hardware and software. Clause 5.5 of the MS ISO/IEC 17025 standards also applies to both hardware and software including the test tools.

5.6 Measurement traceability

In ITSET, calibration of test equipment refers to identifying the suitability of a test tool for a particular use, where calibration is not required, a process of verification shall take precedence.

Any test tools used to conduct security evaluations that are not part of the unit under evaluation shall be studied in isolation to make sure they correctly represent and assess the test assertions they make. This equipment shall also be examined to make sure they do not interfere with the conduct of the test and do not modify or impact the integrity of the product under test in any way. Laboratories shall have procedures that ensure appropriate configuration of all test equipment. Laboratories shall maintain records of the configuration of test equipment and all analysis to ensure the suitability of test equipment to perform the desired testing.

For CC testing, “traceability” refers to security evaluation activities which are traceable to the underlying CC requirements and work units in CEM. This evaluation methodology demonstrates that the tests conducted and the tests assertion made are traceable to CC and CEM to ensure that test results constitute credible evidence of compliance with CC and CEM.

5.7 Sampling

Within the context of ITSET, sampling may refer to test case selection which include:

a) Selection of test cases to different conditions and combination variables
b) Selection of regression tests to rerun
c) Selection of source code to review based on risk

Sampling records for testing conducted shall be maintained which may include:

a) Test case selection

b) Justification of the test case selection

c) Test Plan

5.8 Handling of test and calibration items

The interactions between the test items, the test tools and the test environment may result in modification to the TOE as part of the normal installation or testing process. The laboratory shall protect products under evaluation and verified tools used for the evaluation from any modification, unintended use or unauthorised access. For evaluated product which include software component, the laboratory shall ensure that the configuration management mechanisms are in place to prevent unintended modifications to the software components during the evaluation process. Procedure to ensure proper retention, disposal or return of software and hardware after the completion of the evaluation shall be established and maintained.

5.9 Assuring the quality of test and calibration results

The laboratory shall participate in relevant Proficiency Testing program where available.

Assurance of quality test shall be performed at identified intervals throughout the evaluation process. In MyCC Scheme, this should be performed through Technical Review meetings between Laboratory, and MyCB.

5.10 Reporting the results

The laboratory shall issue evaluation reports of its work that accurately, clearly and unambiguously present the evaluator analysis, test conditions, test setup, test and evaluation results and all other required information. Evaluation reports shall provide all necessary information to permit the same or another laboratory to reproduce the evaluation and obtain comparable results.

For the purpose of complying with MyCC requirements, two types of evaluation report shall be produced:

a) 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 MyCC Scheme. ETR shall be submitted to MyCB under the MyCC Scheme for review.

b) Evaluation Observation Report (EOR), a report that will **only** be issued by the laboratory once a problem that can potentially affect the assurance of the evaluation is detected. The content of the EOR shall conform to the requirements of relevant policy document under MyCC Scheme. EOR shall be submitted to the developer/sponsor for rectification.

The use of SAMM Accreditation Symbol in both ETR and EOR shall confined to the requirements stated in SAMM Policy 3.

Acknowledgements

1. Ms. Siti Mariam Mohd Din (Chairman)	STANDARDS MALAYSIA
2. Ms. Wong Fei Ting (Secretary)	STANDARDS MALAYSIA
3. Ms. Norhazimah Abdul Malek	CyberSecurity Malaysia
4. Mr. Mohd Zahari Zakaria	Teknimuda (M) Sdn. Bhd.
5. Mr. Shaharil Abd Malek	SCAN Associates Berhad
6. Ms. Norziana Jamil	MIMOS Berhad