CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science, Technology and Innovation

MyCC Scheme Evaluation Facility Manual (MyCC_P3)

File name: MyCB-5-MAN-1-MyCC_P3
Version: v1
Date of document: 23 December 2009
Document classification: PUBLIC

For inquiry about this document,
please email to mycc@cybersecurity.my

For general inquiry about us or our services,

please email: info@cybersecurity.my

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8945 3205

Level 7, Sapura@Mines
No. 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia

www.cybersecurity.my

Securing Our Cyberspace

MyCC Scheme Evaluation Facility Manual (MyCC_P3)

23 December 2009

MyCB Department

CyberSecurity Malaysia

Level 7, Sapura@Mines No 7 Jalan Tasik

Mines Resort City 43300 Seri Kembangan, Selangor

Tel: +60 (0)3 8992 6888 Fax: +60 (0)3 8945 3205

http://www.cybersecurity.my

Forward

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been established under the 9th Malaysian Plan to increase Malaysian competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) established within CyberSecurity Malaysia.

This document defines the evaluation requirements for MySEFs operating under the MyCC Scheme. The requirements defined in this document apply to all MySEFs.

Husin Jazri

Chief Executive Officer

CyberSecurity Malaysia

All correspondence in connection with this document should be addressed to:

Scheme Manager

MyCB Department

CyberSecurity Malaysia

Level 7, Sapura@Mines

No 7 Jalan Tasik

The Mines Resort City

43300 Seri Kembangan

Selangor, Malaysia

Document Authorisation

DOCUMENT TITLE:	MyCC Scheme Evaluation Facility Manual (MyCC_P3)
DOCUMENT REFERENCE:	MyCB-5-MAN-1-MyCC_P3
ISSUE:	v1
DATE:	23 December 2009

DISTRIBUTION:	UNCONTROLLED COPY

Copyright and Confidentiality Statement

Registered office:

Level 7, Sapura@Mines,

No 7 Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan,

Selangor, Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Trademarks

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalized. CyberSecurity Malaysia cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Disclaimer

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and CyberSecurity Malaysia shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this document.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
v1	23 Dec 2009	All	Final released. Update format, cover, document identifier, document classification, document authorisation and content based on previous version P07001-CND-011 MyCC Evaluator Manual 1.1, 30 June 2008

Table of Contents

Index of Tables

Index of Figures

.

1 Introduction

1.1 Purpose

1 This manual (**MyCC_P3**) that provides interpretation of the MyCC Scheme Policy (**MyCC_P1**) as applied to the management and operation of licensed Malaysian Security Evaluation Facilities (MySEFs).

2 The intended audience for this document is the Scheme manager, MySEF Lab Managers, certifiers and evaluators. More information on the operation of the MyCC Scheme, and the conduct of certification and evaluation activities, can be found in other MyCC Scheme publications at www.cybersecurity.my/MyCC. The other official MyCC Scheme publications are:

a. The MyCC Scheme Policy (**MyCC_P1**) that provides an overview of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme and specifies the business rules governing its operation as a member of the Common Criteria Recognition Arrangement (CCRA);

b. The MyCC Scheme Certified Products Register (**MyCC_P2**) that lists all certifications and evaluation projects; and

c. The MyCC Scheme Customer Manual (**MyCC_P4**) that provides guidance to sponsors, developers and consumers of certified products.

3 Other official publications that provide detailed guidance for aspects of MyCC Scheme operation that are not publicly available are:

a. The MyCC Scheme Certification Manual (**MyCC_P5**) that provides interpretation of this policy application for the management and operation of the MyCC Scheme and the Malaysian Common Criteria Certification Body (MyCB); and

b. The MyCB Quality Manual (**MyCB_QM**) that defines the management system for operation of the Malaysian Common Criteria Certification Body (MyCB).

4 Third parties seeking access to documents that are not publicly available must submit a request in writing to the MyCC Scheme. The decision to release these documents to a third party is at the discretion of the MyCC Scheme and may be subject to conditions as part of that release.

1.2 Scope

5 This manual applies to the operation of every Malaysian Security Evaluation Facility (MySEF) licensed to conduct evaluations under the MyCC Scheme and MyCC Scheme customers.

1.3 Document Organisation

6 This policy document is organised into the following sections:

a. **Section One** provides an introduction to the manual outlining its purpose, scope, authority, document organisation and related publications.

b. **Section Two** describes the minimum requirements to become and maintain operation as a licensed MySEF within the MyCC Scheme, and the application process.

c. **Section Three** provides an overview of the workflow and functions for each business process associated with the delivery of evaluation services by a MySEF.

d. **Section Four** contains the description of the workflow and functions for the PLAN function of an evaluation in a MySEF.

e. **Section Five** contains the description of the workflow and functions for the EXECUTE function of an evaluation in a MySEF.

f. **Section Six** contains the description of the workflow and functions for the CLOSE function of an evaluation in a MySEF.

g. **Section Seven** contains the description of the workflows and functions for each assurance process applicable to a MySEF.

h. **Section Eight** contains a description of the interfaces with MyCB processes applicable to MySEF operations.

i. **Annex A** contains the Terminology and definitions relevant to MySEF management and evaluation services.

1.3.1 Document Relationships

7 The relationship between the MyCC Scheme Evaluation Facility Manual (shown in red) and other documents in the hierarchy is illustrated in Figure 1 below.

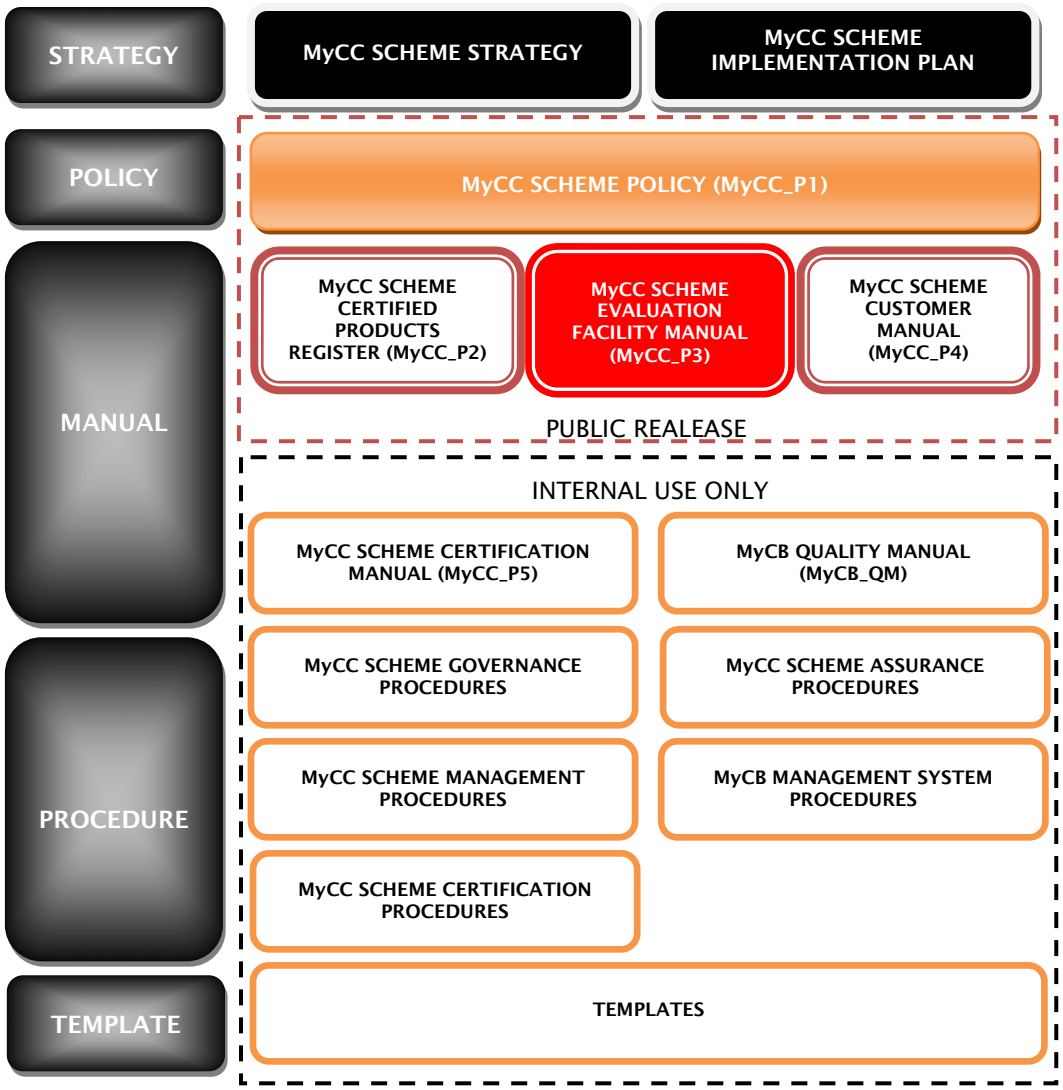


Figure 1: Document Relationships

1.4 Changes to this Manual

8 The change authority for the MyCC Scheme Evaluation Facility Manual is the MyCC Scheme Head. All change requests in relation to the manual should be forwarded in writing to the Scheme Manager.

9 All changes will be submitted to the MyCC Scheme Management Board for final approval.

10 All approved changes to the MyCC Scheme Evaluation Facility Manual will be published on the www.cybersecurity.my/MyCC website.

2 MySEF minimum requirements

11 This section describes the requirements that are required to be met for an organisation to become a MySEF and to maintain their licence. The staffing requirements, accreditation requirements, application process and maintenance requirements are described separately in the following subsections.

2.1 MySEF staffing

12 Each licensed MySEF is required to maintain, as a minimum, the following roles:

a. MySEF Lab Manager;

b. Senior MySEF Evaluator;

c. MySEF Evaluator; and

d. MySEF Quality Manager.

13 While one person can fill more than one role, the MySEF is required to maintain a minimum of two staff to ensure that appropriate reviews are performed.

14 Figure 2 provides a graphical representation of the hierarchy of these roles. Each role, and the associated minimum education and professional experience requirements are described in subsections 2.1.1, 2.1.2, 2.1.3 and 2.1.4.

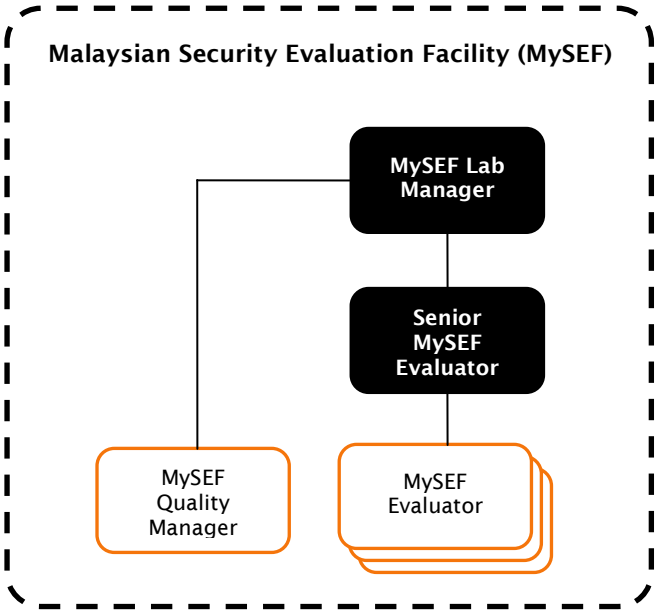


Figure 2: MySEF Role Structure

2.1.1 MySEF Lab Manager

15 The MySEF Lab Manager role is responsible for the general management of MySEF personnel, and the relationship and interface with the MyCB. This role may be an authorised MS ISO/IEC 17025 signatory. While one person can fill more than one role, each MySEF will have only one staff member nominated as the MySEF Lab Manager.

16 The MySEF Lab Manager is required to have the following knowledge and skills:

a. Formal project management qualifications (e.g. PRINCE2, PMBOK);

b. MS ISO/IEC 17025 and its application to MySEF operations;

c. MySEF Management System; and

d. Business Management.

17 Ideally, the MySEF Lab Manager will also have evaluation skills equivalent to the Senior MySEF Evaluator role.

2.1.2 Senior MySEF Evaluator

18 The Senior MySEF Evaluator role reports to the MySEF Lab Manager and is responsible for:

a. Ensuring the effective application of ICT security evaluation criteria for evaluations conducted within the MySEF;

b. The technical development of MySEF evaluators in the facility;

c. The continuous application of the MySEF Management System to the conduct of evaluations within the MySEF; and

d. Acting as an MS ISO/IEC 17025 authorised signatory for evaluation work.

19 The Senior MySEF Evaluator is required to have the following knowledge and skills in addition to those required of a MySEF Evaluator:

a. At least two years Common Criteria evaluation or certification experience;

b. Formal project management qualifications (e.g. PRINCE2, PMBOK);

c. MS ISO/IEC 17025 and its application to MySEF operations;

d. Recognised as an Authorised signatory for STANDARDS MALAYSIA; and

e. MySEF Management System.

20 While one person can fill more than one role, each MySEF will have only one staff member nominated as the Senior MySEF Evaluator.

2.1.3 MySEF Evaluator

21 The MySEF Evaluator is responsible for the conduct of day-to-day evaluation projects under the direction of the Senior MySEF Evaluator and in compliance with the MySEF Management System.

22 MySEF evaluators are required to have pre-requisite knowledge and skills in at least one of the following areas:

a. Software engineering;

b. Electronics engineering;

c. Microcontroller architecture and programming;

d. ICT Security; and

e. Systems Analysis.

23 Pre-requisite knowledge can be demonstrated by tertiary qualifications, professional certifications, or equivalent experience in at least one of those areas identified in Table 1 below before they can conduct ICT security evaluation work.

Table 1: Evaluator Basic Qualifications and Certifications

Qualification	Description
ICT Degree	Bachelor, Masters or PhD in information and communication technology that includes at least one but not limited to the following: • Software engineering • Microcontroller architecture and programming • Systems analysis and design • Security
Computer Science Degree	Bachelor, Masters or PhD in computer science that includes at least one but not limited to the following: • Software engineering • Computer architecture • Microcontroller architecture and programming • Systems analysis and design • Security
Electronics Engineering Degree	Bachelor, Masters or PhD in electronics engineering that includes at lease one but not limited to the following: • Microcontroller architecture and programming • Digital electronics • Analogue electronics
CISSP	Certified Information System Security Professional

Qualification	Description
SSCP	Systems Security Certified Practitioner – Only where the evaluator has an indirectly related degree. For example if an evaluator has a degree in business information systems, then SSCP is suitable to augment their skills for ICT security evaluation.

2.1.4 MySEF Quality Manager

24 This role is responsible for maintenance of the MySEF Management System, and conducts reviews of the application of the management system within the MySEF.

25 The MySEF Quality Manager is required to have the following knowledge and skills:

a. MS ISO/IEC 17025 and its application to MySEF operations; and

b. Comprehensive understanding of the MySEF Management System.

26 Ideally, the MySEF Quality Manager will also have one or more of the following skills:

a. Formal project management qualifications (e.g. PRINCE2, PMBOK); and

b. ICT and Management System Audit (Certified Information System Auditor, ISMS Lead Auditor or equivalent).

27 While one person can fill more than one role, each MySEF will have only one staff member nominated as the MySEF Quality Manager.

2.1.5 Project Specific Roles

28 Within each project, there are two key roles, in addition to team members. The MySEF should nominate a Lead Evaluator and at least one Authorised Signatory for each project. The nomination will be contained in the Evaluation Project Plan. One person may fill both of these roles.

Lead Evaluator

29 The Lead Evaluator is the technical lead and project manager for a given evaluation project. They are responsible for ensuring that the Common Criteria requirements are met, and that the project meets the proposed schedule within the proposed budget.

30 In addition to being an evaluator, the Lead Evaluator for a project is required to have the following experience:

a. Equivalent knowledge of the product type to the attackers defined in the Security Target;

b. Participated in all evaluation aspects of the proposed evaluation level, during at least two evaluations; and

c. Formal project management qualifications (e.g. PRINCE2, PMBOK).

Authorised Signatory

31 The Authorised Signatory for a project is responsible for authorising all reports and documents that are produced during an evaluation project. They are required to ensure that the evaluation is conducted in accordance with MS ISO/IEC 17025.

32 In addition to being an evaluator, the Authorised Signatory for a project is required to have the following experience/qualifications:

a. MS ISO/IEC 17025 and its application to MySEF operations;

b. Recognised as an Authorised Signatory for STANDARDS MALAYSIA; and

c. At least two years Common Criteria evaluation or certification experience.

2.1.6 Allocation of Roles

33 The MyCB is responsible for approving the allocation of MySEF staff to MySEF Roles, based on their qualifications. The MySEF Lab Manager is responsible for nominating MySEF staff for roles, and providing a justification that the nominated staff member is skilled appropriately to perform the Role.

2.2 MySEF Application

34 Any company wishing to become a MySEF is required to complete an application proposal outlined in section 2.2.1, and meet the requirements specified in section 2.2.2 and 2.3.

35 Applicants are required to pay a non-refundable application fee to MyCB for assessing the application. The current fee structure is published on the www.cybersecurity.my/MyCC website.

2.2.1 Application Proposal

36 The application proposal is composed of four parts. Part 1 of the application proposal requires information about the organisation seeking a MySEF license. Part 2 requires a statement of organisational capability and structure. Part 3 requires specific details of the proposed resources of the MySEF. Part 4 is a statement of compliance against the draft license agreement. An overview of the information required on each part of the proposal is provided below.

Part 1 - Organisation information:

a. Corporate entity, name, address and legal status; and

b. Details of any potential or existing conflict of interest that would affect the applicant's ability to become a MySEF or to perform the functions of a MySEF.

Part 2 - Statement of claims:

a. Organisation background and structure;

b. Financial capacity to support ICT security evaluation services;

c. Curriculum vitae of proposed evaluation staff and MySEF roles;

d. Staff experience using ICT security evaluation related skills, such as experience in the use of formal methods or functional and vulnerability testing;

e. Details of MS ISO/IEC 17025 accreditation, or a plan for how it will be achieved;

f. The management structure that will achieve and maintain the quality, security and confidentiality of ICT security evaluations;

g. The organisation's quality assurance system;

h. An outline quality plan for the conduct of ICT security evaluations;

i. A plan for supervision of inexperienced evaluators; and

j. Any other supporting factors to support the application.

Part 3 - Facilities and infrastructure:

a. Proposed MySEF accommodation;

b. Proposed physical and logical security arrangements;

Part 4 – Statement of Compliance to MySEF Licence Agreement

a. Compliance statement for each clause of the licence agreement; and

b. Justification for any non-compliance.

2.2.2 MS ISO/IEC 17025 Requirements

37 For a new MySEF, MS ISO/IEC 17025 accreditation is required to be completed either:

a. Prior to the submission of their final evaluation technical report (ETR) for their first completed evaluation project; or

b. Within twelve (12) months of being granted their MySEF license,

whichever is the sooner.

2.2.3 Submitting the Application

38 An applicant is required to submit **three (3)** hard copies and **one (1)** electronic copy (CD-ROM) to the Scheme Manager at the address shown on the MyCC Scheme web-site (www.cybersecurity.my/MyCC).

39 The MyCB will notify receipt of an application to become a MySEF and if there are any deficiencies in the application material. An applicant has **five (5)** business days to address any deficiencies and resubmit its application.

2.2.4 Assessment of Application

40 The MyCB is responsible for assessing an application to become a MySEF. Assessment includes review of the application and the conduct of a site visit by an assessment team appointed by the MyCB. The MyCB will provide notification of the site visit to the applicant during the assessment process.

41 During the assessment, the MyCB may require additional information to clarify or confirm claims made in the evaluation application. The applicant is required to provide additional information in a timely fashion.

2.3 Operational Requirements

42 A MySEF is required to maintain accreditation to MS ISO/IEC 17025 (Ref [1]) throughout their license period. The scope of accreditation for MS ISO/IEC 17025 must include the following evaluation services:

a. **Security evaluation of CC Protection Profiles (PP), and ICT products and systems (called a target of evaluation (TOE))** – Impartial assessment of the security of a TOE against a set of functional and assurance claims using ISO/IEC 15408 (Ref [2]) and ISO/IEC 18045 (Ref [3]) and in conformance with MyCC Scheme Policy (Ref [4]).

43 A licensed MySEF is required to deliver these services in accordance with the following:

a. MyCC Scheme Policy (MyCC_P1) (Ref [4]);

b. This manual – Evaluation Facility Manual (MyCC_P3);

c. ISO/IEC 15408 The Common Criteria for IT Security Evaluations (Ref [2]);

d. ISO/IEC 18045 The Common Evaluation Methodology (Ref [3]); and

e. Their MS ISO/IEC 17025 (Ref [1]) accredited management system.

44 The MySEF should implement appropriate security controls to ensure confidentiality of customer information, and to ensure that evaluations are unaffected by other projects taking place in the MySEF.

45 MySEF personnel are required to sign a confidentiality undertaking prior to their commencement in any role within their MySEF.

3 Evaluation Overview

46 All evaluations occurring under the MyCC will be performed in three functions: Plan, Execute, and Close. These functions and their relationships to the MyCC are outlined in Figure 3.

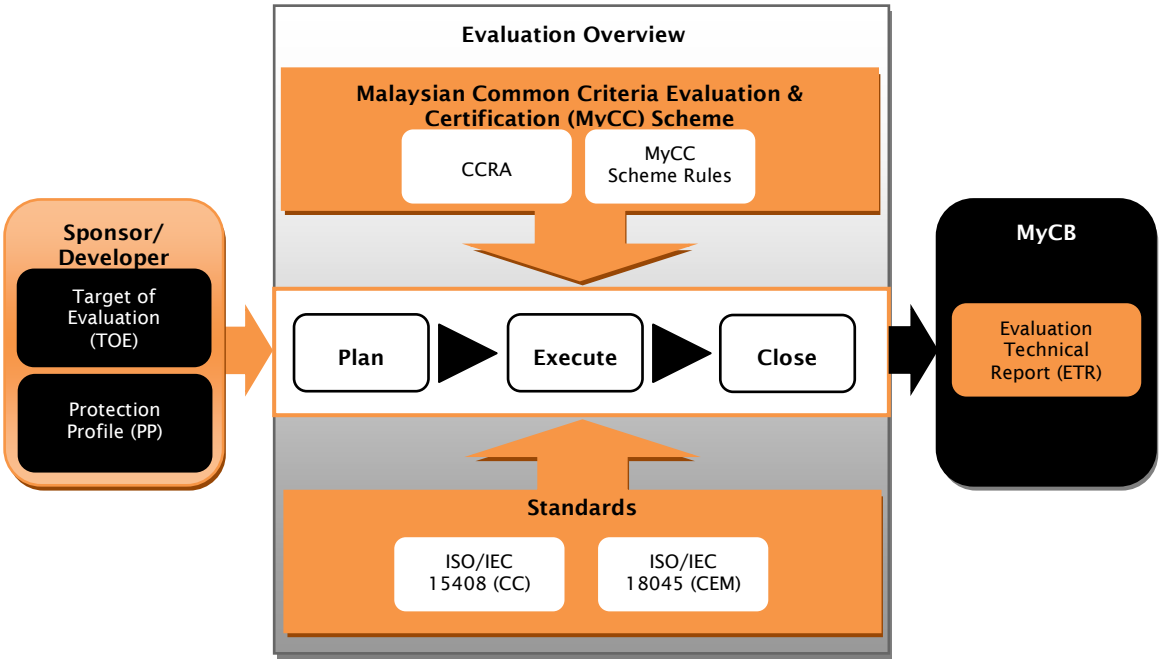


Figure 3: Evaluation Overview

3.1 Plan

47 This function is the commencement of each evaluation that occurs in the MySEF. The purpose of the function is to ensure that each evaluation has a sound base and that the evaluation has a reasonable chance of completion.

3.2 Execute

48 The focus of the MySEF in this function is to determine whether the TOE provides the functionality claimed and whether the claimed CC requirements have been met.

3.3 Close

49 This function allows customers of the MySEF to provide feedback on the evaluation process, and formally ends the evaluation.

4 Plan

50 The following flow chart[1] shows the activities of the evaluation planning function.

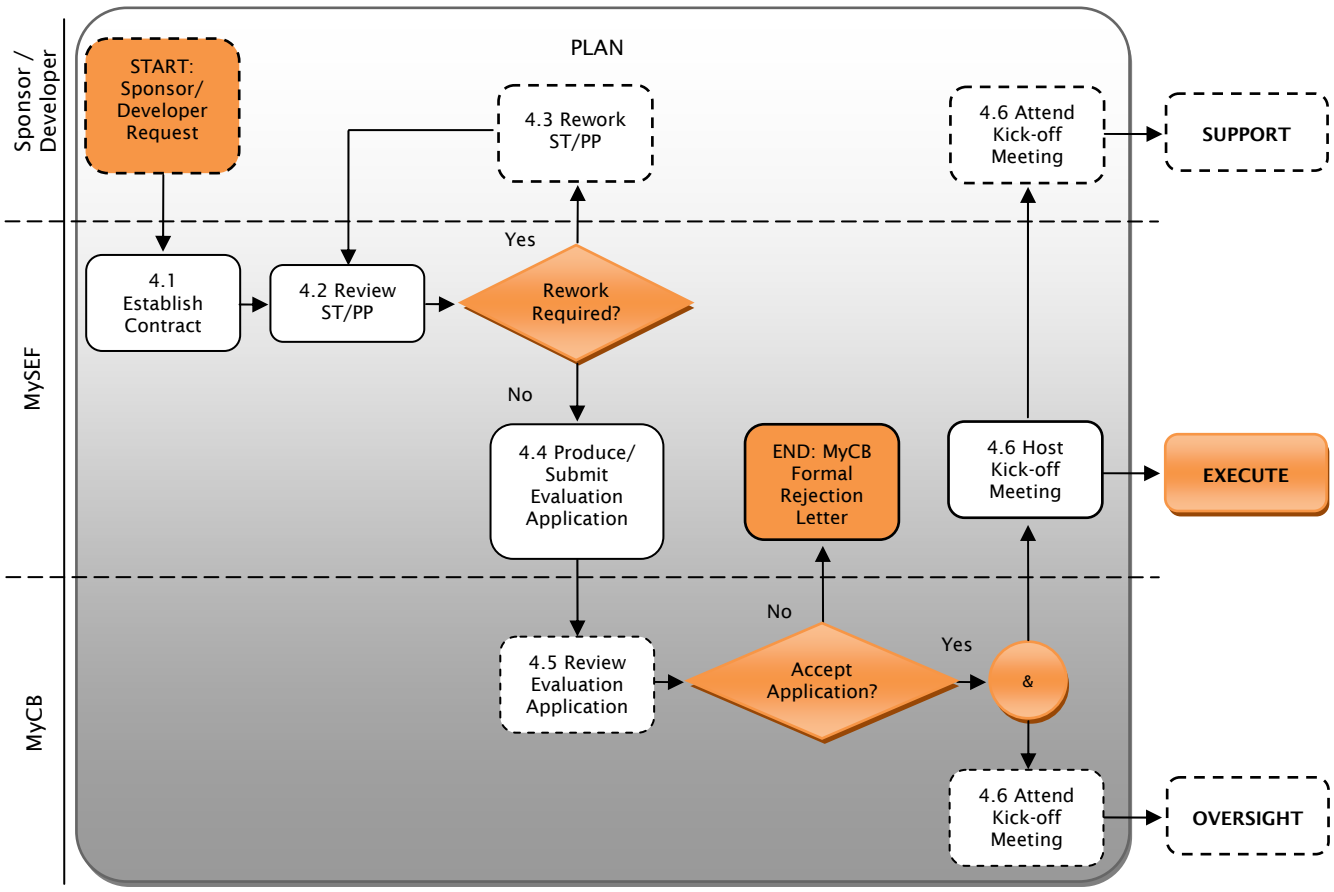


Figure 4: Plan

4.1 Establish Contract

51 Prior to the commencement of any evaluation work, the MySEF Lab Manager will ensure that a contract to provide the evaluation services is in place. The contract will assign the MySEF as their authorised representative for engaging with MyCB.

52 The MySEF Lab Manager will ensure that the sponsor is aware of their responsibilities as described in the MyCC Scheme Customer Manual (MyCC_P4).

[1] Flow chart conventions are described in Annex A.3

4.2 Review ST/PP

53 The Senior MySEF Evaluator is required to review the Security Target or Protection Profile to determine whether it is a sound basis for evaluation. Note: The MySEF is not expected to evaluate the Security Target or Protection Profile at this stage, only determine whether the Security Target is complete, and that the scope of the TOE is clearly defined and reasonably consistent with the included SFRs. If the Security Target or Protection Profile is not complete at this stage, the MySEF can provide informal comments to assist the developer in developing a suitable Security Target or Protection Profile.

4.3 Rework ST/PP

54 If the MySEF has comments on the initial Security Target or Protection Profile, the sponsor/developer will be requested to address the comments and resubmit the Security Target to the MySEF for review.

4.4 Produce/Submit Evaluation Application

55 The MySEF Lab Manager is required to produce an evaluation application to advise the MyCB of the intention to perform an evaluation. The Evaluation Application includes the following documents:

a. Security Target or Protection Profile that forms the basis of the evaluation;

b. A statement of any potential or actual conflict of interest that arises as a result of the MySEF conducting the evaluation and any proposed measures to manage that conflict of interest;

c. The MySEF must ensure that the sponsor and the developer (if applicable) are aware of their responsibilities to support the evaluation. The MySEF should provide evidence that the sponsor/developer has acknowledged these responsibilities; and

d. An Evaluation Project Proposal.

4.4.1 Evaluation Project Proposal

56 The Evaluation Project Proposal is required to contain the following information:

a. Evaluation project scope – the project scope includes key details of the evaluation, including the TOE Name and Version, CC Version and Assurance Level, any applicable National and International Interpretations released at the time of writing, and an overview of the TOE functionality.

b. Contact details for all stakeholders – this includes the Point of Contact details for the developer, sponsor and Lead Evaluator.

c. Evaluation resources – resource assignment must include a summary of the evaluation teams experience and a justification of the sufficiency of the team. This section is required to nominate a Lead Evaluator and at least one Authorised Signatory for the project.

d. Schedule and work-breakdown structure – this section will divide the evaluation into manageable pieces and provide estimated commencement and completion dates for each piece of work; and

e. Proposed confidentiality requirements – this should include communication between the MyCB, MySEF, sponsor and developer. Requirements may also be specified in a confidentiality agreement between two or more parties for an evaluation project. Confidentiality requirements should include the measures to be used for the storage and transmission of information between the parties to the agreement.

f. Proposed reuse of results from previous evaluations – this section is required to demonstrate that the reuse of results is appropriate, and that the previous results are relevant to the proposed TOE.

4.4.2 Notes for Reuse of Evaluation Results

57 Where a MySEF intends to reuse past evaluation results, the MySEF is required to organise a re-evaluation planning meeting (RPM). The RPM is attended by:

a. A MySEF representative;

b. A MyCC Scheme Certifer;

58 The MySEF is required to distribute the agenda for an RPM **five (5)** business days prior to the meeting with the following additional inputs where applicable and available:

a. An IAR report that considers the impact of changes on the assurance baseline of the certified TOE;

b. The ST for the current TOE (for re-evaluation);

c. The ETR for the certified TOE[2];

d. The CR for the certified TOE[3]; and

e. The MySEF rationale for reuse of evaluation results.

4.5 Review Evaluation Application

59 The MyCB will review the evaluation application within **ten (10)** business days of receipt of the Evaluation Application by the MyCC Scheme and advise the MySEF and the sponsor whether the application has been accepted. If the MyCB finds any deficiencies in the evaluation application, then the MySEF has **two (2)** business days to address these deficiencies and resubmit the evaluation application. If the evaluation is accepted, the Kick-off Meeting is held. If the application is rejected, the evaluation process ends.

[2] The MyCB will normally have access to the ETR for the original certified TOE – this need not be provided by the MySEF.

[3] The MyCB will normally have access to the CR for the original certified TOE – this need not be provided by the MySEF.

4.6 Host Kick-off Meeting

60 Once formally accepted by the MyCB, the MySEF Lead Evaluator for the evaluation is required to organise an Evaluation Kick-off Meeting. The kick-off meeting is attended by:

a. The certifier(s) assigned by the MyCB to the evaluation project;

b. The lead evaluator for the evaluation project;

c. A representative of the sponsor; and

d. A representative of the developer.

61 The agenda for the meeting include at least the following points:

a. Overview of the scope of the TOE;

b. Overview of the evaluation process;

c. Overview of the roles and responsibilities;

d. Agreement to the schedule; and

e. Confirm confidentiality requirements.

5 Execute

62 The following flow chart shows the progress of the execute function of an evaluation.

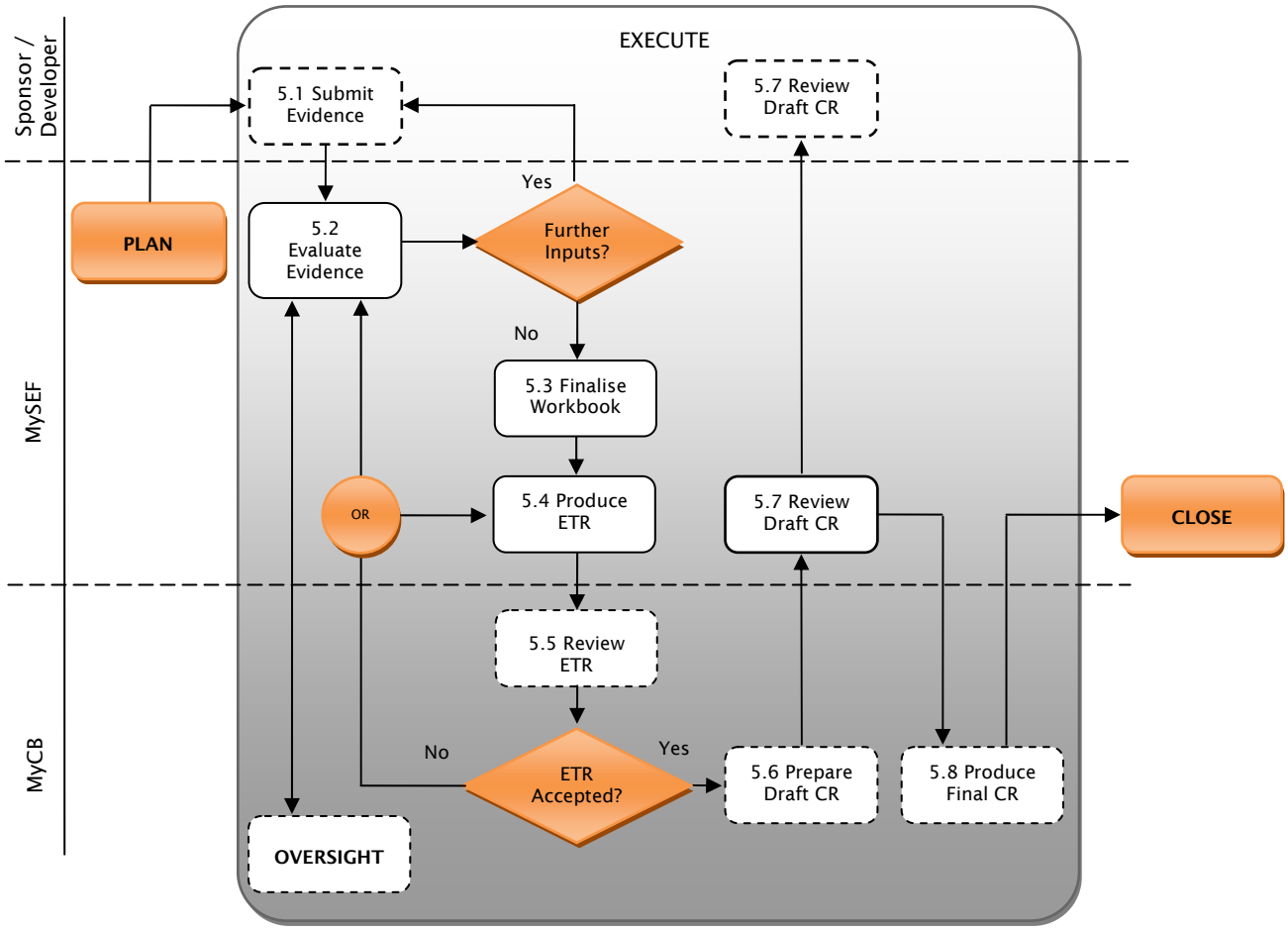


Figure 5: Execute

5.1 Submit Evidence

63 The sponsor/developer is required to provide evidence to the MySEF that meets the requirements of the Common Criteria for the assurance requirements defined in the Security Target or Protection Profile.

5.2 Evaluate Evidence

64 The MySEF is required to apply the requirements outlined in the Common Criteria and Common Evaluation Methodology, to the evidence provided by the developer. This Activity is outlined in Figure 6 and described in the subsections following.

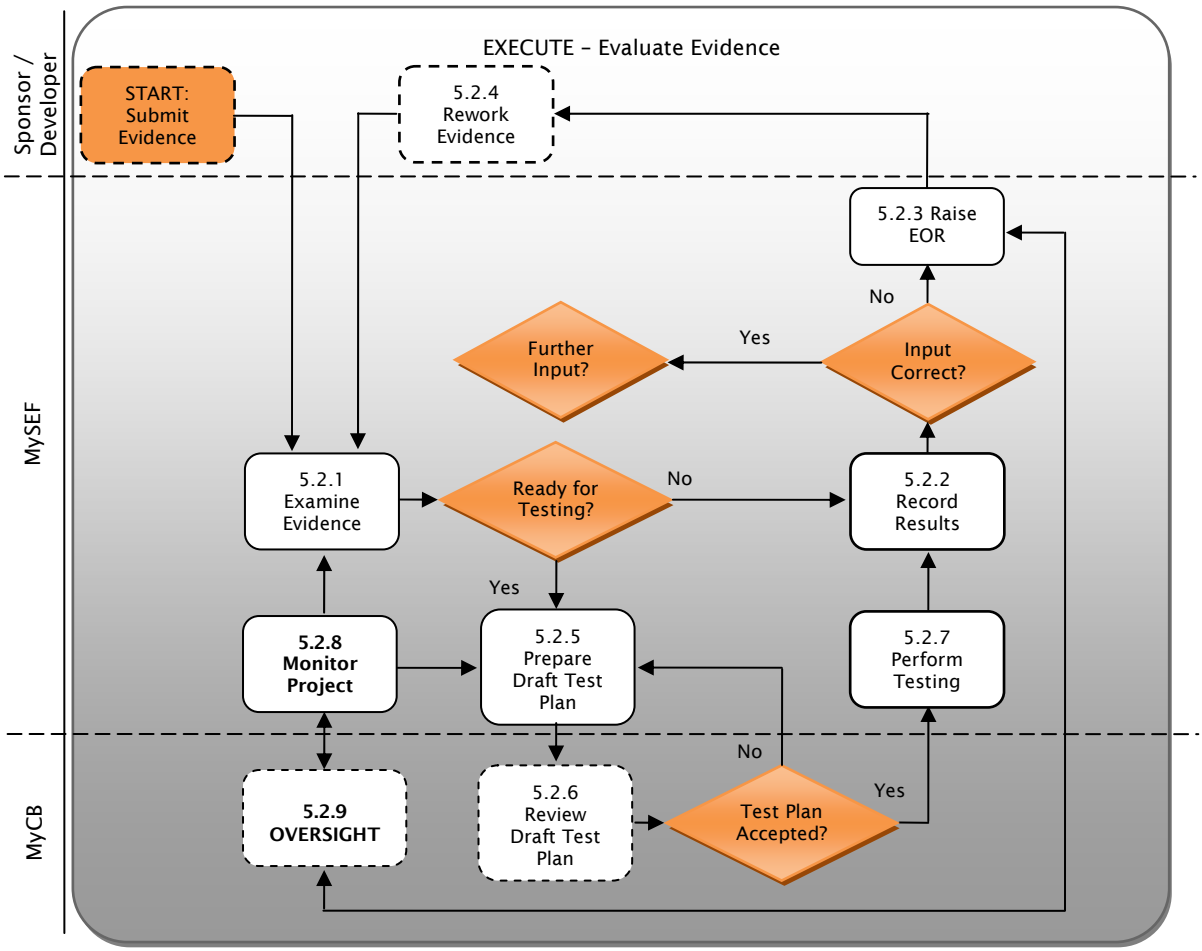


Figure 6: Evaluate Evidence

5.2.1 Examine Evidence

65 For each assurance requirement claimed in the Security Target or Protection Profile, the MySEF evaluators are required to apply the CC (Ref [2]), CEM (Ref [3]) and any interpretations agreed at the Kick-off Meeting to determine that the evidence supplied meets the requirements. The MySEF evaluators may also apply interpretations made after the Kick-off meeting, subject to agreement from the sponsor and the Lead Certifier.

Note: It is not a requirement that any specific document aside from the Security Target or Protection Profile exists, e.g. there does not have to be a document called “Functional Specification” as long as the CC requirements are met by one or more of the documents submitted for evaluation.

5.2.2 Record Results

66 The MySEF evaluators are required to evaluate the evidence in accordance with the Evaluator Action Elements described in the Common Criteria Evaluation Methodology (Ref [3]).

67 The MySEF evaluators are required to record the result of the evaluation in the Evaluator Workbook.

68 The MySEF evaluators are also required to assign verdicts to the requirements of the security evaluation criteria, that is ‘pass’, ‘fail’ or ‘inconclusive’.

5.2.3 Raise EOR

69 The MySEF evaluators are required to raise an Evaluation Observation Report (EOR) once a problem that can potentially affect the assurance of the evaluation is detected. Note that evaluator is not permitted to use an EOR to raise any non-assurance related issues with the sponsor.

70 An EOR contains the following information:

a. Identifier assigned to the evaluation project to which the EOR relates to;

b. Unique reference number of the EOR;

c. Version number of the EOR;

d. Date on which the EOR was raised;

e. Details of the evaluation action element against which the issue was found and the relevant work package;

f. Details of the evaluation deliverables that are relevant to the EOR;

g. Observation – describe the problem being reported in sufficient detail to provide the MyCB and the sponsor understanding to the nature of the problem and its implications;

h. EOR Resolution – detail the resolution of the problem, this section evolves as the resolution takes place.

i. Authorisation Section – detail the authorisation by relevant parties for the release and/or resolution of the EOR.

71 The MySEF may include, the following information, as required:

a. Implication – identify the implication for the problem raised to the evaluation (e.g. an indication of potential knock on effects);

b. Recommendation – provide general advice on how the problems can be solved. Note: MySEF evaluators on a project cannot contribute to the development of the TOE and therefore cannot provide detailed recommendations for remediation of observations.

72 EORs will be provided to the sponsor and Lead Certifier. The Lead Evaluator is required to advise the Lead Certifier if the EOR describes a potential vulnerability.

5.2.4 Rework Evidence

73 The developers are required to provide the MySEF evaluators with resolutions to all raised EORs in accordance with the MyCC Customer Manual (MyCC_P4). Evaluation evidence will be submitted to the MySEF for review.

5.2.5 Prepare Draft Test Plan

74 During the execution of the evaluation, the Lead Evaluator will be required to submit test plans for:

a. The conduct of development site visits;

b. The conduct of functional testing; and

c. The conduct of penetration testing.

Site Visits

75 When the Lead Evaluator is ready to plan for a site visit, the evaluators are required to prepare a draft test plan. The test plan is required to meet the requirements defined in the CEM and will include the following details:

a. Date(s) and site(s) for the site visit;

b. Key personnel involved in the site visit;

c. Purpose of the proposed site visit, including requirements that need to be addressed;

d. Details of the development site personnel that will be interviewed during the site visit and their role in the TOE development;

e. For each assurance requirement that will be tested during the site visit:

i. The reference documentation satisfying the assurance requirement;

ii. The proposed action that will be taken at the site visit to verify the assurance requirement has been satisfied;

f. For each interview that will be conducted:

i. The details of the individual that will be interviewed;

ii. Planned timings for the interview and who will conduct the interview;

iii. A list of interview questions and potential follow-up questions;

76 The test plan is to be submitted at least **five (5)** working days and approved by MyCB prior to the commencement of testing.

Functional and Penetration Testing

77 When the Lead Evaluator is ready to plan for testing, the evaluators are required to prepare a draft test plan. The test plan is required to meet the requirements defined in the CEM and will include the following details:

a. Date(s) and site(s) of testing;

b. Key personnel involved in the testing effort;

c. Purpose of the proposed testing effort, including requirements that need to be addressed;

d. Test environment, including the version or configuration of the TOE, hardware and software components including their version numbers and configuration settings;

e. Test specifications for each test that is going to be performed. The test specification should identify:

i. Objective of the test – including a justification for the test. This may include a reference to a problem report or other evaluation records;

ii. Cross references to applicable security functional requirements (Only for functional testing);

iii. Steps involved – detail of steps that are going to be performed by the evaluators in conducting the test, identifying inputs and configuration settings; and

iv. Expected or desired results.

78 The test plan is to be submitted at least **five (5)** working days and approved by MyCB prior to the commencement of testing.

5.2.6 Review Draft Test Plan

79 The MyCB is required to review and respond within **five (5)** working days of receipt of the test plan. Review of the test plan is required to be performed in accordance with MyCC Certification Manual (MyCC_P5).

80 If the test report is accepted, the MySEF evaluators can commence testing. If the MyCB has comments, the Lead Evaluator will address the comments in a new draft of the test plan.

5.2.7 Perform Testing

81 The MySEF evaluators are required to record the results throughout the testing. The following information must be recorded for each test:

a. Date the test was performed;

b. Evaluators involved in performing the test;

c. Any additional information relevant to the performance of the test; and

d. Results obtained from the test.

82 At the completion of testing, the MySEF evaluators are required to compare the results obtained from the execution of the test with the expected test results detailed in the test plan. Any deviation from the expected results must be documented and accounted for.

83 Vulnerabilities that are discovered during testing must be reported to the MyCB in accordance to Section 5.2.3 above.

5.2.8 Monitor Project

84 Project monitoring occurs throughout the Evaluate Evidence function, and consists of the following aspects.

Evaluation Progress Report

85 The Lead Evaluator is required to report progress of the evaluation by submitting Evaluation Progress Report each month to MyCB.

86 The report will include at least the following points:

a. An overview of the project against the agreed schedule;

b. Previous evaluation activities –activities that have been recently completed;

c. Upcoming evaluation activities – to identify future evaluation activities. The Lead Certifier may also provide the evaluation team with guidance for the upcoming evaluation activities; and

d. Overview of the EORs – including the status of issued EORs.

e. Project risks and issues and any planned activities to address these risks and issues

Project Progress Meeting

87 The Lead Evaluator is responsible to conduct a formal meeting between the certification team, evaluation team and the sponsor to discuss matters related to the execution of an evaluation project when required. If required, evaluation team, certification team or sponsor can request from the Lead Evaluator for the project progress meeting.

5.2.9 Oversight

88 The MyCB is responsible to conduct this function as described in the MyCC Scheme Policy (MyCC_P1) and MyCC Scheme Certification Manual (MyCC_P5). Within the OVERSIGHT function, the certification team perform the technical certification work and utilise this phase to gain a greater understanding of the TOE and to oversee evaluation activities. This function comprises the following aspects.

Technical Review Meeting

89 The MyCB is responsible for organising regular technical review meetings to discuss the technical aspects of the evaluation. The planned frequency of these meetings will be identified in the formal acceptance correspondence provided by the MyCB to the MySEF and the customer. At a minimum assurance technical review meeting will be attended by:

a. The lead certifier assigned by the MyCB to the evaluation project; and

b. The lead evaluator for the evaluation project.

90 To conduct this meeting, the MyCB may request evaluator evidence of work undertaken on an evaluation project be provided to the lead certifier prior to the technical review meeting and/or during the technical review meeting.

Oversight the Testing

91 Lead Certifier (or their delegate) is responsible to review and approved the test plans prior to the commencement of testing as described in Section 5.2.6. The test plans include the development site visit plan, functional and penetration testing plan.

92 During execution of the development site visit, functional and penetration testing activities for an evaluation project, the Lead Certifier (or their delegate) may attend the activities as observer.

Handle Observation Report

93 During the execution of the evaluation project, the Lead Evaluator will provide information copies of all evaluation observation reports (EORs) generated in accordance to Section 5.2.3. In general EORs fall into two categories:

a. Evaluation inputs. EORs that relate to non-compliance of evaluation inputs with CC requirements. In the main, these result from documentation review; and

b. Vulnerabilities. EORs that relate to exploitable vulnerabilities identified by the evaluation team. In the main, these result from functional and/or penetration testing.

94 The certification team receives these EORs to monitor for exploitable vulnerabilities identified by the evaluation team. Where an exploitable vulnerability is discovered, MyCB may elect to suspend the evaluation project until a remediation strategy can be agreed with the sponsor.

Monitor Evaluation Project

95 Lead Certifier is responsible to monitor the evaluation project progress based on the Evaluation Progress Report provided monthly by the Lead Evaluator as described in Section 5.2.8. If issues raised during the evaluation met the suspension or termination criteria as described in the MyCC Scheme Policy (MyCC_P1), MyCB may suspend or terminate the evaluation project.

5.3 Finalise Evaluator Workbook

96 The MySEF evaluators are required to finalise the workbook. This includes performing an internal review of the workbook in accordance with the MySEF implementation of MS ISO/IEC 17025.

5.4 Produce ETR

97 The MySEF evaluators are required to document their findings in an Evaluation Technical Report (ETR), which represents the final output from the evaluation project. The conclusions documented in the ETR state the degree to which the evaluation criteria and security functionality have been met, with supporting evidence. The ETR content needs to conform to the requirements of the evaluation methodology, and MS ISO/IEC 17025, and is required to be submitted by the MySEF to the MyCB for review.

5.5 Review ETR

98 The MyCB is required to review the ETR submitted by the MySEF evaluator to ensure that all evaluation requirements have been adhered to.

99 Acceptance of the ETR by the MyCB is required prior to the release of CR.

5.6 Prepare Draft CR

100 The MyCB is required to produce a Certification Report (CR) which reflects the results of the evaluation. The MyCB will provide the draft CR to the Lead Evaluator and customer for review.

5.7 Review Draft CR

101 The drafted CR is reviewed by the MySEF Lead Evaluator for the project and the customer to ensure that the information contained within the report accurately reflects the TOE and the evaluation work performed.

102 The MySEF Lead Evaluator is required to submit a set of comments from the evaluator and the sponsor to the MyCB within **five (5)** working days of receiving the draft Certification Report.

5.8 Produce Final CR

103 Once received the comments from MySEF Lead Evaluator, the MyCB is responsible produce a revised version that is submitted to the MyCC Scheme Certification Subcommittee for final approval and issue of the certificate for the evaluation.

6 Close

104 This section describes the functions of the Close function of an evaluation. Figure 7 provides an overview of the flow of the Close function.

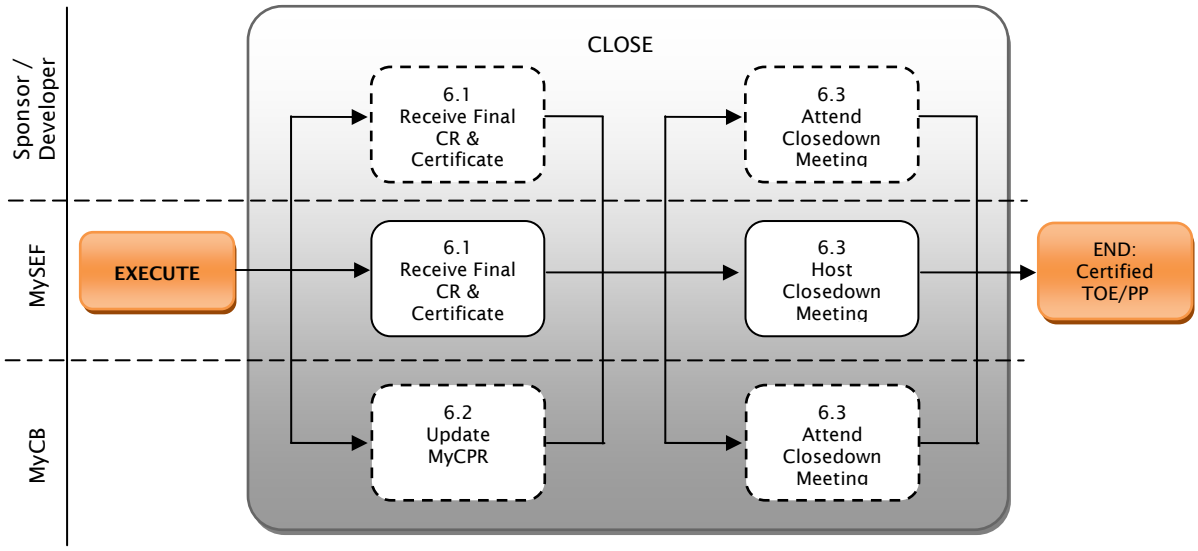


Figure 7: Close

6.1 Receive Final CR and Certificate

105 The MyCB will provide a copy of the final Certification Report and Certificate to the MySEF and the sponsor. The MySEF is required to archive the Certification Report with the other evaluation records.

6.2 Update MyCPR

106 Once the final version of the CR has been approved, the MyCB is required to publish the details of the evaluation project, its certification report and other supporting documentation as required by the CCRA on the MyCC Scheme Certified Product Register (MyCPR) (www.cybersecurity.my/MyCC/MyCPR.html) and the Common Criteria portal (www.commoncriteriaportal.org) to reflect the certification of the TOE.

6.3 Host Closedown Meeting

107 Once the TOE is certified and the final Certification Report is received, a formal closedown meeting will be hosted by the MySEF conducting the evaluation project. The evaluation closedown meeting is required to be attended by:

a. The certifier(s) assigned by the MyCB to the evaluation project;

b. The lead evaluator for the evaluation project; and

c. A representative of the sponsor.

108 The meeting will include at least the following points:

a. Summary of the evaluation, including key dates;

b. Time to complete evaluation and certification activities;

c. Effort spent in the delivery of evaluation and certification services;

d. Vulnerabilities discovered and corrected through the delivery of evaluation and certification services;

e. Consumer and customer satisfaction with the evaluation and certification services offered by the scheme; and

f. Confirm confidentiality and archiving requirements.

7 MySEF Assurance Process

109 This section provides a description of the workflows and functions for each assurance process applicable to a MySEF. The processes that will be included are:

a. Operate MySEF Management System;

b. MySEF Management Reporting for the MyCC Scheme; and

c. Liaison with Third Party MyCC Scheme MySEF Auditors.

7.1 Operate MySEF Management System

110 This process defines, maintains, monitors and improves the MySEF management system in accordance with MS ISO/IEC 17025 requirements of ICT testing facilities.

111 Prospective MySEFs should contact STANDARDS MALAYSIA regarding MS ISO/IEC 17025 accreditation.

7.2 MySEF Management Reporting for the MyCC Scheme

112 The process for collating the outcomes of (continuous and planned) assurance activities related to a MySEF(s) and for the preparation and delivery of management-level reports to the MyCC Scheme Head (as required) and to senior management of the MySEF(s). This will occur at least annually and is part of maintaining MS ISO/IEC 17025 accreditation. This process incorporates two key functions:

a. Monitor MySEF Key Performance Indicators; and

b. Prepare MySEF Business Report.

7.2.1 Monitor MySEF Key Performance Indicators

113 The MySEF is required to monitor (as a minimum) the following key performance measures and report performance in the MySEF Business Report:

a. Time to complete evaluation activities;

b. Effort spent in the delivery of evaluation services;

c. Vulnerabilities discovered and corrected through the delivery of evaluation services;

d. Consumer and customer satisfaction with the evaluation services offered by the scheme;

e. Outcomes of management reviews and accreditation activities undertaken;

f. Training and development activities undertaken by the evaluators; and

g. Any other aspects and indicators as directed by the MyCC Scheme owner.

7.2.2 Prepare MySEF Business Report

114 The MySEF Business Report shall be prepared and submitted to the MyCB on an annual basis, outlining the following information:

a. **Prospective business**: The MySEF provides the MyCB with details of contacts made with prospective clients, allowing the MyCB to gauge the level of demand for MyCC services and to understand potential future certifier and resource requirements.

b. **Staffing**: A list of all current MySEF staff members, and their current status or roles within the MySEF. This should include an indication of the percentage of time, against full time equivalence, that each staff member is allocated to MySEF activities. This section of the report should also highlight any changes in personnel or their status since the previous MySEF Business Report.

c. **Licensing and accreditation status**: The report indicates the current state of the MySEF licensing and accreditation status, highlighting any changes since the previous MySEF Business Report. Any STANDARDS MALAYSIA accreditation reports will also be discussed.

d. **Scheme issues**: Any general issues in relation to the MyCC Scheme that the MySEF may wish to bring to the attention of the MyCC Scheme are to be included in the report.

e. **Key Performance Indicators**: The MySEF shall report on the KPI's, including any changes since the previous MySEF Business Report.

115 The Scheme Manager may request a meeting with the MySEF Lab Manager to discuss matters arising from the business report.

7.3 Liaison with Third Party MyCC Scheme MySEF Auditors.

116 This process for assisting third party reviewers (External and Independent) with the conduct of their responsibilities associated with assessing the operation of the MySEF. This process incorporates two key functions:

a. Assist CCRA Expert Reviewers; and

b. Assist MyCC Scheme Auditors.

7.3.1 Assist CCRA Expert Reviewers

117 The MyCC Scheme is required to participate in CCRA Voluntary Periodic Assessment activities every five years. This may require the MySEF to allow access to evaluation facilities, projects and staff by technical experts to facilitate reviews of the MyCC Scheme by external experts in the CCRA.

7.3.2 Assist MyCC Scheme Auditors

118 All MySEFs are required to submit to an audit by the MyCB upon receipt of written notice on intention to conduct an audit by the MyCB. MyCB audits are not scheduled and may be conducted for reasons including:

a. A customer complaint;

b. An appeal of a certification decision;

c. As a result of MS ISO/IEC 17025 accreditation issues;

d. As a result of reported Shadow Certification/Voluntary Periodic Assessment issues; and/or

e. As a random activity.

119 The MySEF is required to provide any assistance to MyCC Scheme Auditors that is reasonably requested in auditing the MySEF.

120 In addition to MyCB audits, a MySEF is required to maintain accreditation against MS ISO/IEC 17025. Accreditation requires periodic assessment by STANDARDS MALAYSIA appointed assessors. MySEF Lab Managers should contact STANDARDS MALAYSIA for the schedule of these assessments. The MySEF is required to provide any assistance to assessors that are reasonably requested in completing accreditation.

8 Interfaces with MyCC Scheme and MyCC Scheme Certification Body processes

121 The following table shows the interfaces between MyCC Scheme Business Processes and the Certification Business Processes, and the MySEF roles. The table also details for each interface, the information exchanged and the timing.

Table 2: MyCC Scheme Interfaces to MySEF

MyCC Scheme and Certification Business Processes	MySEF Roles				Project Roles	
	MySEF Lab Manager	MySEF Senior Evaluator	MySEF Quality Manager	MySEF Evaluator	Lead Evaluator	Authorised Signatory
MyCC Scheme Industry Engagement	MyCC Scheme Change Request (As needed)					
MyCC Scheme Policy and Standards						
MyCC Scheme Risk Management						
MyCC Scheme Legal Services	Execute MySEF License Agreement (Commencement of MySEF)					
MyCC Scheme Marketing and Promotion	MySEF Business Report (Annually)					

MyCC Scheme and Certification Business Processes	MySEF Roles				Project Roles	
	MySEF Lab Manager	MySEF Senior Evaluator	MySEF Quality Manager	MySEF Evaluator	Lead Evaluator	Authorised Signatory
MyCC Scheme Secretariat Services						
Publications Management						
MySEF Management	MySEF Business Report (Annually) Attendance at meetings to discuss business report		Monitoring performance against KPIs Assisting MS ISO/IEC 17025 assessors			
CC Interpretations Management		MyCC Interpretation Request (As needed) Attendance at meetings to discuss national interpretations and technical evaluation issues.				
CCRA Engagement	Participate in VPA (every 5 years)	Participate in VPA (every 5 years)	Participate in VPA (every 5 years)	Participate in VPA (every 5 years)		

MyCC Scheme and Certification Business Processes	MySEF Roles				Project Roles	
	MySEF Lab Manager	MySEF Senior Evaluator	MySEF Quality Manager	MySEF Evaluator	Lead Evaluator	Authorised Signatory
CC Training and Development	Attend Training Execution (as needed)	Attend Training Execution (as needed)	Attend Training Execution (as needed)	Attend Training Execution (as needed)		
Certify Evaluation Results	Acceptance Documentation (for each project)				Evaluation Progress documentation (monthly for each project)	Environment Assessment and testing Plans (for each project) Evaluation Technical Report (for each project)
Maintain Certificate						
Recognise Certificate						

Annex A Reference Material

A.1 References

[1] MS ISO/IEC 17025 – The General Requirements for the Competence of Testing and Calibration Laboratories, International Standards Organisation, 2005.

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

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

[6] Assurance Continuity, CCRA Requirements, Version 1.0, February 2004.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

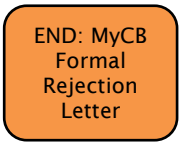
Acronym	Expanded Term
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CEO	Chief Executive Officer
CR	Certification Report
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
ICT	Information and Communications Technology
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target
TOE	Target of Evaluation

A.3 Flow Chart Conventions

A.3.1 MySEF Activities

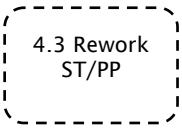
122 Activities that must be performed directly by the MySEF are represented by a white box with a solid outline.

123 Activities that must be performed directly by the MySEF and represent end of activity for current function or phase are represented by an orange box with a solid outline.



A.3.2 Other Activities

124 Activities that are related to the evaluation workflow but are not performed by the MySEF are represented by a white box with a dashed outline.



125 Activities that are related to the evaluation workflow but are not performed by the MySEF and represent start activity for current function or phase, are represented by an orange box with a dashed outline.

A.3.3 External Function/Phase/Activity

126 Functions, Phases and Activities that occur outside of the current function or phase are represented by a box filled with orange. These boxes represent predecessors or successors to the current function or activity.

A.3.4 Decision

127 Decision points are represented by a diamond. Decision points are graphical representations of a decision that is made in the activity preceding the decision point.

--- END OF DOCUMENT ---