MyCC Scheme Customer Manual (MyCC_P4)

File name: ISCB-5-MAN-2-MyCC_P4
Version: v1b

Date of document: 24 November 2015

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)
Best Brand Internet Security 2008 & 2009
MS ISO/IEC 17021: 2011 ISMS 02082013 CB 02
Status Company
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

MyCC Scheme Customer Manual (MyCC_P4)

24 November 2015

ISCB Department

CyberSecurity Malaysia

Level 5, 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), a scheme established in Information Security Certification Body department within CyberSecurity Malaysia.

This document provides guidance to MyCC Scheme customers including sponsors of ICT security evaluations and consumers of certified ICT products and systems.

Dr Amirudin Abdul Wahab

Chief Executive Officer

CyberSecurity Malaysia

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

Scheme Manager

ISCB Department

CyberSecurity Malaysia

Level 7, Sapura@Mines

No 7 Jalan Tasik

The Mines Resort City

43300 Seri Kembangan

Selangor, Malaysia

DISTRIBUTION: UNCONTROLLED COPY

Copyright and Confidentiality Statement

Registered office:

Level 5, 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	25 January 2010	All	Final released. Update format, cover, document identifier, document classification, document authorisation and content based on previous version P07001-CND-017 MyCC Customer Manual 1.0, 22 Oct 2008
v1a	24 November 2014	All	Update header, footer, document authorisation, document reference
v1b	24 November 2015	Figure 1, Annex A.1	Update header, footer, document authorisation, document reference.

Table of Contents

Index of Tables

Index of Figures

.

1 Introduction

1.1 Purpose

1 This publication (**MyCC_P4**) provides:

a. Information on evaluation and certification processes to stakeholders external to the MyCC Scheme to assist them in supporting evaluation and certification of their product, system or protection profile within the MyCC Scheme; and

b. Guidance for users of certified products in relation to the secure delivery, configuration and use of those products.

2 This guidance is aligned with the rules for evaluation and certification defined in the MyCC Scheme Policy (Ref [6]).

1.2 Scope

3 This publication provides general guidance to evaluation sponsors, developers and consumers of certified products. It is expected that this publication will be read in conjunction with the MyCC Scheme Policy (Ref [6]).

4 Readers should contact the MyCC Scheme via the contact details published at www.cybersecurity.my/mycc if they have specific questions in relation to the information provided in this, or any other, MyCC Scheme publication or in relation to the MyCC Scheme Certified Products Register (MyCPR).

1.3 Document Organisation

5 This document is organised into the following sections:

a. **Section One** provides an introduction to the manual, including a description of its purpose and scope.

b. **Section Two** provides an overview of the certification and evaluation process.

c. **Section Three** provides guidance for sponsors of evaluation projects in the MyCC Scheme.

d. **Section Four** provides guidance to consumers of MyCC Scheme certified products.

e. **Section Five** provides an overview of the Common Criteria.

f. **Annex A** lists the references and terminology relevant to the MyCC Scheme Customer Manual.

1.3.1 Document Relationships

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

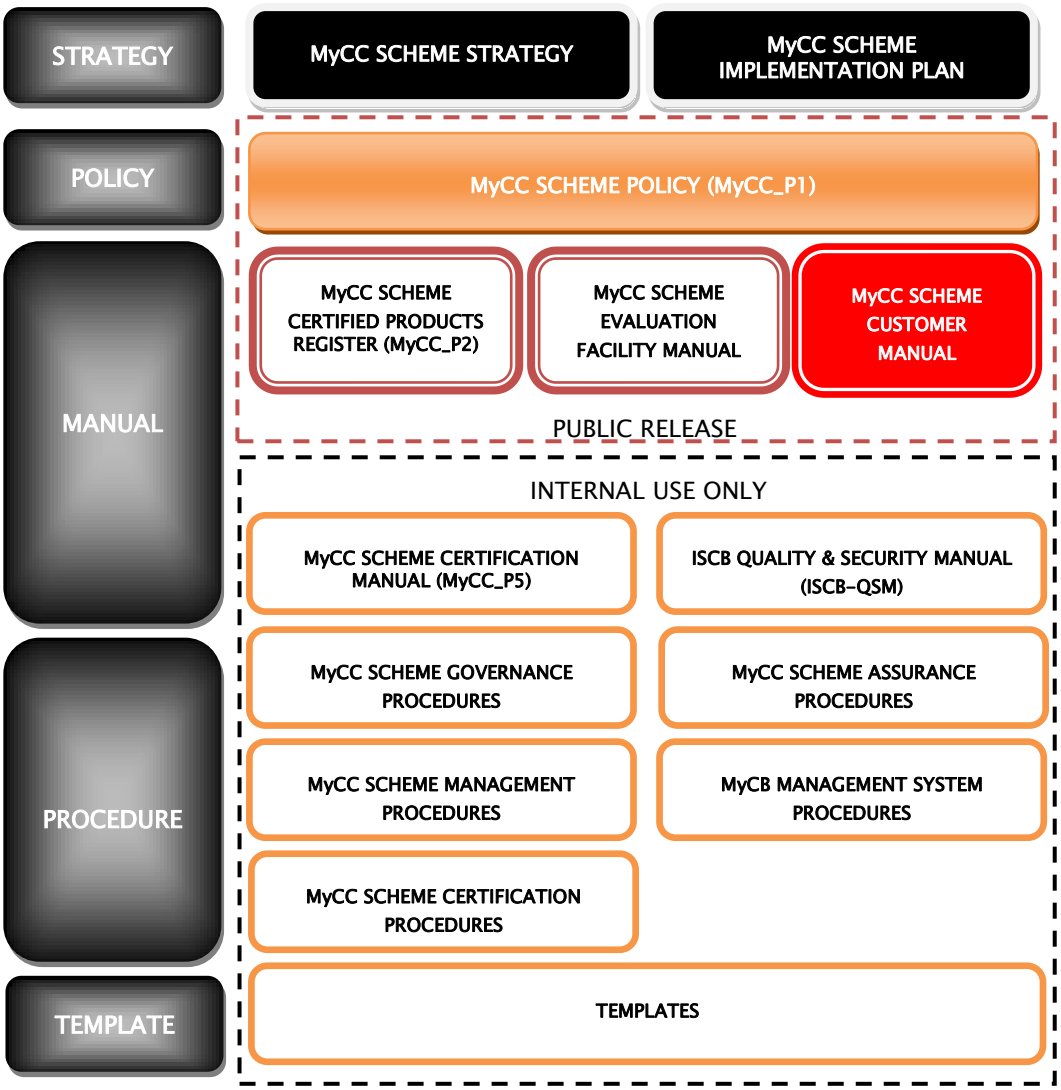

Figure 1: Document Relationships

1.4 Changes to this Manual

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

8 All approved changes to the MyCC Scheme Customer Manual will be published on the www.cybersecurity.my/mycc website.

2 The Certification and Evaluation Process

2.1 Stakeholders

9 There are five stakeholders in the certification and evaluation process:

a. **Developer:** Developer of the product or system under evaluation, which is referred to as the Target of Evaluation (TOE). Alternatively, this stakeholder may also be the developer of a Protection Profile (PP) that is under evaluation. The developer is primarily responsible for the production of evaluation evidence. The developer may also be required to support an evaluation project at key points including:

i. Facilitation of development site visits;

ii. Provision of test equipment; and

iii. Provision of expert training.

b. **Sponsor:** Provides the evaluation evidence to the MySEF for evaluation and establishes the contractual relationship for the evaluation of a product, system or protection profile with the MySEF. A sponsor may also be the **developer**.

c. **Evaluator:** Performs evaluation of the product, system or protection profile in accordance with the IT security evaluation criteria and methodology.

d. **Certifier:** Provides oversight of the application of the IT security evaluation criteria and methodology by the **evaluator**.

e. **Consumer:** Acquires and uses certified products within their IT environment.

2.2 Role of the MyCC Scheme

10 The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme was established in December 2007 under the 9th Malaysian Plan. Its mission is ***to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products***.

11 The MyCC Scheme is operated by CyberSecurity Malaysia as a component of its security assurance services. An overview of the structure of the MyCC Scheme is illustrated Figure 2 below.

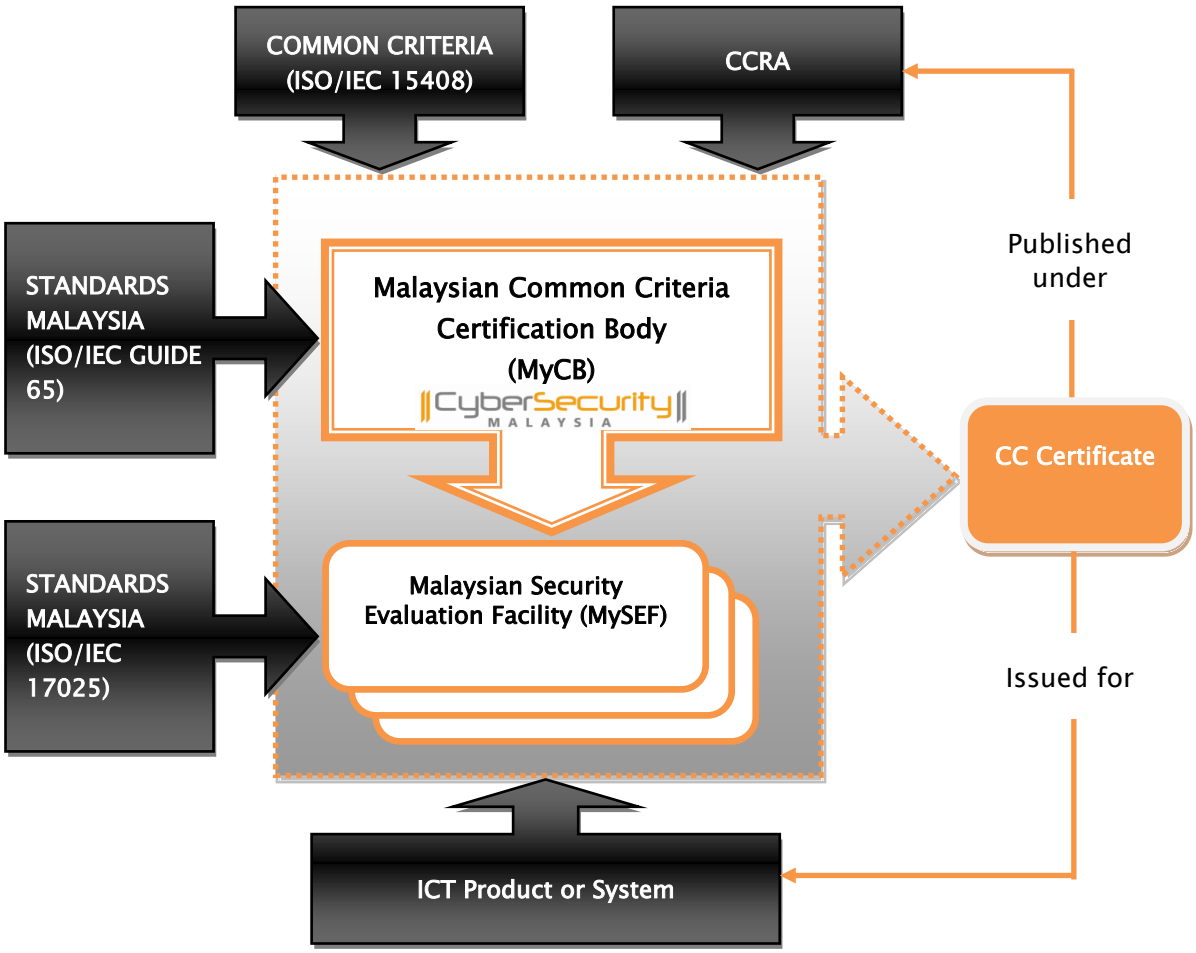

Figure 2: MyCC Scheme Structure

12 The group within CyberSecurity Malaysia that manages the operation of the MyCC Scheme and certifies the results of evaluations is called the Malaysian Common Criteria Certification Body (MyCB).

13 The MyCB licenses organisations, which are known as Malaysian Security Evaluation Facilities (MySEFs), to conduct evaluations under the MyCC Scheme rules. A listing of licensed MySEFs is published at www.cybersecurity.my/mycc.

14 A sponsor initiates the process by engaging a MySEF to evaluate their product, system or protection profile. The MyCB monitors the evaluation process, interacting with evaluators where necessary, and providing independent oversight activities to ensure that the process is conducted in accordance with the requirements of the IT security evaluation criteria, the evaluation methodology and the Common Criteria Recognition Arrangement (CCRA) (Ref [1]). The MyCB issues a certificate for those products and systems that meet the requirements of the IT security evaluation criteria. The overall process is illustrated in Figure 3 below. Please refer to MyCC Scheme Policy (Ref [6]) for the details of the processes and services.

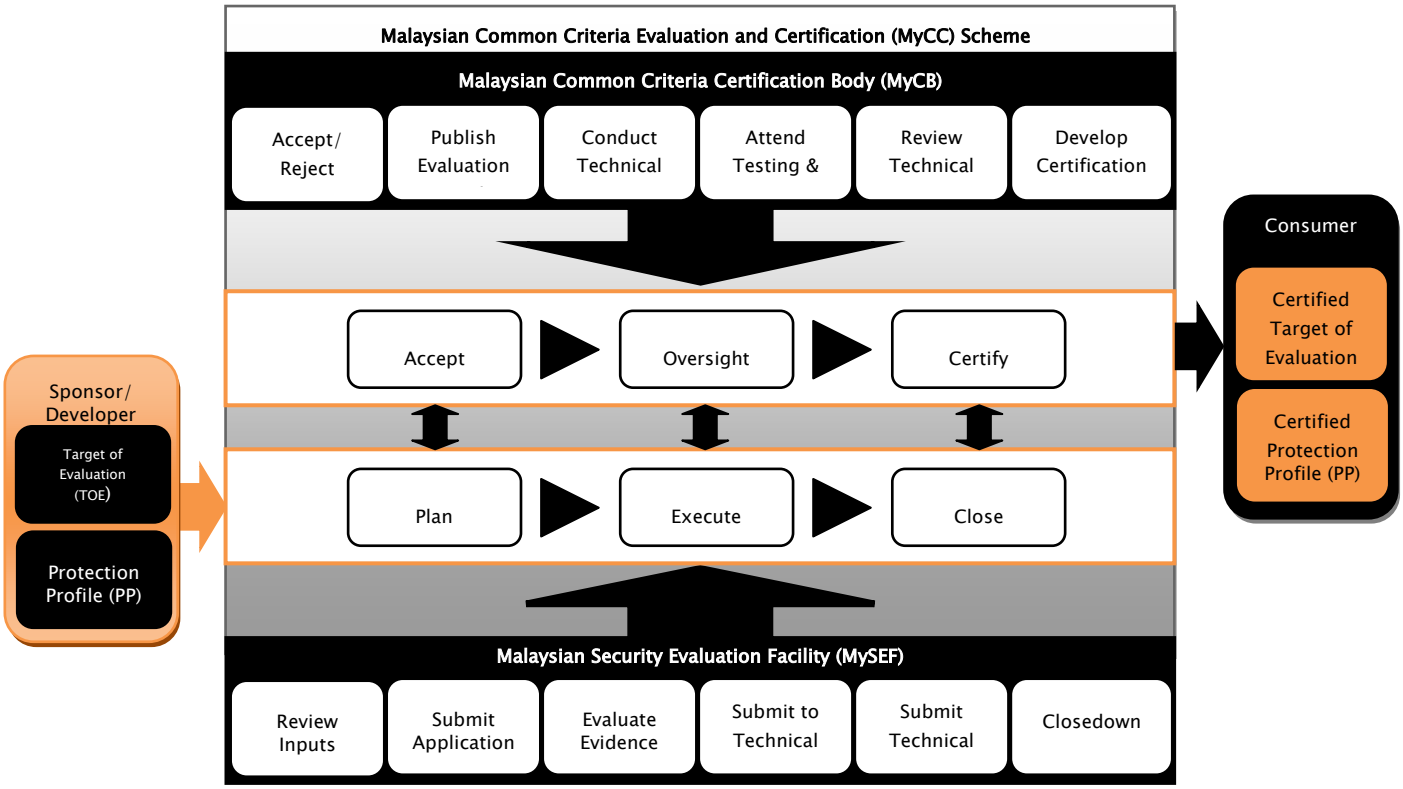

Figure 3: High-level Process of Certification and Evaluation

2.3 Fees for MyCC Scheme Services

15 MySEFs can be contracted by sponsors to conduct evaluations and they charge fees for the TOE and PP evaluation under the MyCC Scheme. **Note:** Sponsors should take care in ensuring that the contractual arrangements are appropriate to their needs as the MyCB will not involve itself in contractual matters between a MySEF and an evaluation sponsor.

16 The MyCB recovers costs for the delivery of MyCC Scheme services through a fee for service charging model. The fee structure for the MyCB component of MyCC Scheme services is published at www.cybersecurity.my/mycc.

2.4 The MyCC Scheme Certified Products Register (MyCPR)

17 The MyCPR provides consumers with details of TOEs and PPs that:

a. Have a current valid certificate under MyCC Scheme rules;

b. Are undergoing evaluation within the MyCC Scheme and have met the criteria for listing; or

c. Have had their certification withdrawn under MyCC Scheme rules.

18 The MyCPR is published at www.cybersecurity.my/mycc/mycpr.html.

2.5 Limitations on Certification and Evaluation

19 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a residual level of risk that exploitable vulnerabilities remain undiscovered in the TOE's claimed security functionality. This residual risk is reduced as the certified level of assurance increases for the TOE.

20 Certification applies only to a specific version of a TOE. Consumers of a certified TOE should make their own risk-based decisions on the use or otherwise of these products or systems.

3 Guidance for Sponsors

3.1 Overview

21 This section provides guidance to sponsors of evaluation projects under the MyCC Scheme. This information is organised as follows:

a. **Protection Profile evaluation:** The benefits of certified protection profiles.

b. **Considering TOE evaluation:** The benefits of a product or system evaluation and the level of commitment required by the sponsor.

c. **Preparing for TOE evaluation:** What a sponsor needs to do when preparing for an evaluation project.

d. **Supporting the TOE evaluation:** What the evaluation and certification process is and what a sponsor needs to do to support a successful outcome.

e. **Maintaining TOE assurance:** How assurance in a certified product or system can be maintained over its lifecycle in a cost-effective manner.

f. **Use of Marks and Notifications:** What the rules are for marketing certified TOEs or PPs and for notifying the MyCB in relation to a TOE or PP that has been certified overseas.

3.2 Protection Profile Evaluation

22 Common Criteria Protection Profiles (PP) provides a means for consumers or communities of interest to express their security needs for a specific TOE type. This can assist with the selection and acquisition of certified products and systems to satisfy those security needs.

23 Potential sponsors for a PP evaluation should consider the following:

a. **Solution independence.** The PP should not specify security requirements with a single product or system solution in mind. This is the role of an ST (See Section 3.4.3)

b. **Set a minimum.** The PP should set the **minimum** security functional requirements to solve the security problem. This should provide greater opportunity for developers to comply with the PP requirements and also for them to add additional security functional requirements if desired.

c. **Align with national security policy requirements.** The PP should use organisational security policies to align the PP requirements with the national security policy requirements for the consumer or community of interest.

d. **Simplicity.** Align the PP to the greatest extent possible with existing Common Criteria security functional requirements and security assurance requirements.

24 A Protection Profile (PP) has a similar structure and content to that of a Security Target (ST) (See Section 3.4.3). However, where the ST describes the implementation characteristics of a specific IT product or system, the PP provides an implementation-

independent statement of security requirements for a specific TOE type – for example a firewall.

25 The advantages of using a PP are:

a. Consumers can express their IT security needs without reference to any specific product or system;

b. Consumers can benchmark different products and systems against a PP whereas it is often difficult to compare product with different STs; and

c. Developers can design their products and systems to meet PP requirements.

3.3 Considering TOE Evaluation

26 Sponsors should consider a number of factors when deciding whether to have a product or system evaluated within the MyCC Scheme including:

a. **Benefits of evaluation:** The benefits to be gained from undertaking an IT security evaluation.

b. **Resource commitment:** The human resources, time, materials and financial costs required to support an IT security evaluation project.

c. **Timeliness:** The typical duration to achieve a successful evaluation outcome.

d. **Selecting the right evaluation target:** The right scope and version of a product or system as the target for an IT security evaluation.

3.3.1 Benefits of Evaluation

27 Independent evaluation of an IT product or system against internationally recognised criteria can bring a number of benefits. These include:

a. **Market Access:** Gaining access to new markets and opportunities in particular to those countries that are a signatory to the Common Criteria Recognition Arrangement. For a list of participating countries, refer to www.commoncriteriaportal.org.

b. **Independent Verification:** Gaining independent verification of security claims in an IT product or system using precise language for product comparison and as a market differentiator.

c. **Vulnerability Management:** Identification and eradication of security flaws discovered during evaluation resulting in a more robust IT product or system; and

d. **Security Engineering Improvement:** Improvement of security engineering practices for IT product or system developers.

3.3.2 Resource Commitment

28 Sponsors will be required to commit resources in preparing for evaluation, throughout the conduct of the evaluation and, in the case of assurance maintenance, after certification of the product or system. A successful evaluation project outcome will depend upon

sufficient human resources, material and finances being committed by the sponsor to the MySEF conducting the evaluation. This level of commitment will vary according to:

a. The agreed scope of the evaluation defined by the Security Target (see Section 3.4.3 for more information on this document) for the product or system entering into IT security evaluation;

b. The type of product or system entering into IT security evaluation; and

c. The assurance requirements for the IT security evaluation (generally defined by the chosen Evaluation Assurance Level (EAL)).

29 In addition to any support provided to the MySEF conducting the evaluation, sponsors are required to provide the following to the **MyCB upon request**:

a. A copy of the evaluation evidence submitted to the MySEF for evaluation;

b. The version of the product or system undergoing evaluation;

c. Test equipment used for functional testing of the product or system; and

d. Technical personnel to assist with establishing a working test environment for the product or system.

30 The MyCB will arrange for the return or disposal of all the material provided at paragraph 29 at the completion of certification unless otherwise agreed between the sponsor and the MyCB.

31 Finally, sponsors are required to pay a fee for certification services to the MyCB unless agreed otherwise between the sponsor and the MyCB. Fees are discussed previously in Section 2.3.

Cost Drivers

32 There are a number of drivers that directly affect costs associated with an evaluation project. These are:

a. **Assurance Level:** The assurance level sought for the evaluation by the sponsor considerably impacts on cost. If a high level of assurance is required:

i. More effort will be expended by the evaluators to determine that the IT product or system meets its stated claims which increases the cost to the sponsor; and

ii. More effort will be needed to complete certification activities in the MyCB, and hence certification fees are higher.

b. **Complexity and evaluation scope:** The complexity, architecture and evaluation scope for the product or system are all factors that generally increase the amount of effort that the evaluators expend to conduct the evaluation. This typically results in higher cost for the sponsor.

c. **Availability of experienced personnel:** Access to personnel with experience in the design, testing, installation and operation of the product or system undergoing IT security evaluation can reduce the evaluator effort required at critical stages of the project. Further, access to personnel who are knowledgeable in the evaluation process and required evaluation evidence can further reduce evaluator effort. This can reduce the evaluation costs.

d. **Reuse of Previous Evaluation Results:** Where a product or system evaluation can make substantial use of previous evaluation results, as agreed in advance with the MyCB, the level of effort can be substantially reduced. This will significantly reduce the evaluation costs for the sponsor. Further information on reuse of previous evaluation results can be found in Section 3.6 on Maintenance of Assurance.

33 A sponsor or developer may elect to outsource the creation of some or all evaluation evidence to consultants with expertise in the IT security evaluation criteria. In particular, inexperienced sponsors may consider using IT security evaluation criteria experts for the production of the Security Target (see Section 3.4.3 on Security Target documents) for their product or system evaluation.

34 **Note:** Where the sponsor does elect to outsource creation of some or all of evaluation evidence, this does not remove the responsibility for the sponsor to provide the evaluation evidence.

3.3.3 Timeliness

35 The decision to enter a product or system into IT security evaluation may be influenced by market opportunity and the demands of consumers. The MyCC Scheme has structured the delivery of services to ensure that evaluation projects are executed and concluded in a time efficient manner. This aim is to ensure that all stakeholders have timely access to a supply of certified products and systems from the MyCC Scheme.

36 The duration of a product evaluation depends on factors including:

a. **Assurance Level:** The assurance level sought for the evaluation by the sponsor impacts on the time to complete the evaluation project. If a high level of assurance is required, the evaluators need to complete additional evaluation activities as the level of assurance increases. This typically increases the duration of the evaluation project.

b. **Project Scope:** Where the sponsor includes a wide range of versions and security functionality, this may increase the level of effort required to complete each required evaluation activity. This typically increases the duration of the evaluation project.

c. **Complexity:** As complexity of the product or system increases, so too can the level of effort required to complete evaluation activities. This typically increases the duration of the evaluation project.

d. **Sponsor experience:** The experience and knowledge of the sponsor in supporting IT security evaluations can greatly influence the duration of the evaluation. As issues are identified with the evaluation evidence the sponsor is required to address these to the satisfaction of the evaluation team. Sponsors with limited experience in IT security evaluation may take long periods to address identified issues and/or produce evaluation evidence, slowing down the progress on the evaluation project.

e. **Reusability of Previous Results:** Where a product or system evaluation can make substantial reuse of past evaluation results, the duration of the evaluation

can be substantially reduced. Further information on reuse of previous evaluation results can be found in Section 3.6 on Maintenance of Assurance.

37 The following table shows target durations to complete evaluation and certification of a product or system without reuse of previous evaluation results. Where substantial reuse of previous evaluation results can be achieved for a product or system, durations may be reduced by more than 50%.

Table 1: Target Evaluation and Certification Duration

Common Criteria Assurance Package	Target Duration
Evaluation Assurance Level 1	4 – 6 months
Evaluation Assurance Level 2	6 – 8 months
Evaluation Assurance Level 3 or 4	8 – 15 months
Evaluation Assurance Level 5 or higher	15 – 24 months

38 The MyCB monitors evaluation project progress against a schedule agreed between all stakeholders early in the evaluation project. It is understood that evaluation projects may require modification of the agreed schedule from time to time catering for unforeseen circumstances. Accepting such variations to the agreed schedule is at the discretion of the MyCB.

39 Sponsors should note that it is the responsibility of the MyCB to reject proposed evaluation projects where any stakeholder is unable to demonstrate that they can commit the necessary resources to meet the agreed schedule.

3.3.4 Selecting the Right Evaluation Target

40 Selecting the right target of evaluation is critical for a successful evaluation project outcome and for realising the maximum return on the evaluation investment. Potential sponsors should consider the following questions in determining the right evaluation target:

a. What version(s) of the Product or System will be evaluated?

b. What will be the evaluation scope?

What Version of the Product or System?

41 One question that may be faced by potential sponsors is what version of a product or system should be the subject of evaluation under the MyCC Scheme. There are two choices:

a. Evaluation of a version of the product or system that currently implemented or available to consumers; or

b. Evaluation of a version of the product or system that is under development or soon to be released.

42 The MyCC Scheme provides no recommendation as to which choice should be selected. However, potential sponsors might wish to consider the following in making their decision:

a. **Can the Product or System Change:** For some products, particularly those already available to consumers, the code base may be frozen by the developer. Evaluation will discover issues with the product or system that may require update to the product or system implementation.

b. **Availability Upon Completion:** For some products or system, particularly those already available to consumers, the product lifecycle may determine that they will no longer be supported or available by the time the evaluation project completes.

c. **Maintenance of Assurance:** Depending upon the development roadmap for a product or system, sponsors may want to have confidence in future versions reducing the costs of future evaluation.

What will be the Evaluation Scope?

43 Potential sponsors should also briefly consider the intended scope of the evaluation of the product or system in developing their business case for evaluation. Potential sponsors might consider the following questions:

a. **How many different versions or variants could be included within the one evaluation project?** There is a considerable level of flexibility in determining the versions or variants of a product or system for an evaluation project. Including a greater number of variants may satisfy the needs of a broader group of consumers without incurring significant additional cost for the evaluation project.

b. **Does my intended market require compliance with one or more PPs or EALs, and does my product or system implement that required functionality?** In some markets, compliance with certified PPs, or a defined EAL is a requirement for that product or system to be procured within a community of consumers. Compliance with a certified PP may also impact the cost and/or duration of the evaluation. Further, a product or system cannot partly comply with a PP, so potential sponsors need to be satisfied that the product or system implements the required functionality.

c. **What security functionality does my market expect to be included for my product or system?** For certain product or systems types, there may be general consumer expectations on the security functionality that should be present. For example, a firewall would be expected to perform filtering of traffic between two or more networks. Potential sponsors should ensure that expected functionality will be included in the evaluation of that product or system. The MyCB generally will not accept an evaluation project that would not meet consumer expectations.

44 Evaluation scope is discussed in more detail in Section 3.4 Preparing for Evaluation.

3.4 Preparing for TOE Evaluation

45 Once a sponsor has reached a decision to submit a product or system to the MyCC Scheme for IT security evaluation, the following steps must be completed:

a. **Formalising Evaluation Arrangements:** Develop the arrangements between the sponsor, the developer and the MyCB, and selection and contracting of the MySEF.

b. **Finalise Evaluation Scope:** Defining the scope and level of assurance for the evaluation through production of the Security Target for the product or system.

c. **Identify Evaluation Evidence:** Identification of other evidence that will be provided to the MySEF for evaluation of the product or system and the schedule for delivery of the evidence.

3.4.1 Formalising Evaluation Arrangements

46 The relationship between the stakeholders for formalising evaluation relationships are highlighted illustrated in the Figure 4 below:

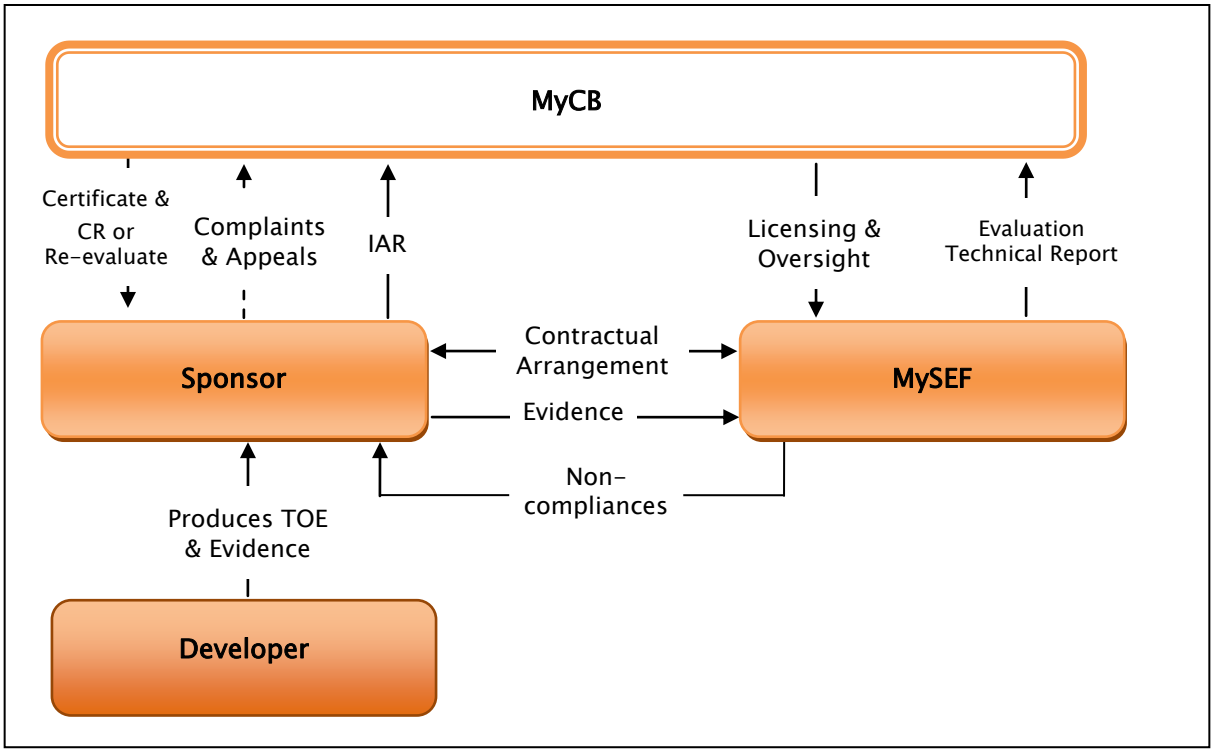

Figure 4: Stakeholder relationships

Sponsor and Developer

47 Typically, the sponsor of an evaluation project is also the developer of the product or system. However, if this is not the case, the sponsor needs to gain, where necessary, the developer's consent to provide required information to the MySEF and/or the MyCB. Sponsors must be able to substantiate that they have the developer's consent to the MyCB upon request.

48 The evidence required for evaluation can include detailed product specifications. At higher levels of assurance, the evaluators and certifiers will require access to source code and/or

hardware drawings for a product or system. The level of detail required will vary depending on the product type and the level of assurance being sought.

Selecting and Contracting a MySEF

49 IT security evaluations are performed by organisations licensed by the MyCC Scheme as competent to perform evaluation projects. An organisation that is licensed to conduct IT security evaluations in the MyCC Scheme is called a MySEF. The sponsor is required to select and contract a MySEF for their evaluation project.

50 The MyCB does not participate in the establishment of contractual arrangements between the sponsor and the MySEF. Sponsors should conduct their own due diligence in selecting a MySEF that aligns with their requirements.

51 **Note:** The MyCB does not set or regulate the fees charged by a MySEF for evaluation services.

52 Sponsors should be aware that IT security evaluation is an iterative process and it is likely that non-compliances with the IT security evaluation criteria will be identified during the evaluation project. It is the responsibility of the sponsor, and not the MySEF, to resolve identified non-compliances in a timely manner so as to not impact the agreed evaluation project schedule. Most MySEFs will establish obligations on the sponsor for the delivery of evaluation evidence to an agreed schedule, and for the timely resolution of identified non-compliances. It is important that the sponsor and the MySEF establish a close working relationship to maximise the likelihood of a successful evaluation project.

53 The MySEF and its proposed team for the evaluation project will:

a. Be knowledgeable on the product or system being evaluated;

b. Have expertise in the IT security evaluation criteria and the evaluation methodology;

c. Conduct the evaluation in accordance with the IT security evaluation criteria and MyCC Scheme Policy (Ref [6]);

d. Report progress and issues to the MyCB in a timely manner;

e. Provide the sponsor with the opportunity to correct identified areas of non-compliance with the IT security evaluation criteria;

f. Respond promptly to direction and oversight provided by the MyCB during the evaluation project;

g. Provide the results of an evaluation project to the MyCB and any matters for consideration by the MyCB for certification of the product or system.

54 The details of licensed MySEFs are published at www.cybersecurity.my/mycc.

The MyCB

55 The MyCB is responsible for acceptance, oversight and certification of all evaluation projects conducted within the MyCC Scheme. Sponsors may request a meeting with

MyCB personnel before establishing a contract with a MySEF for evaluation of their product or system where the sponsors:

a. Want to clarify information provided by the MySEFs on the evaluation process, MyCC Scheme rules and sponsor obligations; and/or

b. To understand opportunities to maximise the value from their proposed product or system evaluation.

56 Once the sponsor has established a contract with a MySEF, the contracted MySEF becomes the first point of contact throughout the evaluation project, unless otherwise directed by the MyCB.

57 In circumstances where the sponsor cannot resolve technical evaluation issues with a MySEF, the MyCB may be contacted for assistance with resolving the issues. The most appropriate mechanism for this resolution is through a Project Progress Meeting called between the stakeholders of the project.

58 **Note:** The MyCB will not involve itself in the resolution of contractual disputes between the sponsor and the MySEF.

59 Sponsors may at any time lodge a complaint or appeal with the MyCB by following the process published at www.cybersecurity.my/mycc.

3.4.2 Determining evaluation scope

60 The sponsor is required to determine the scope of the evaluation prior to commencing the evaluation project. The Security Target (ST) describes the intended operating environment and security requirements for evaluation of the product or system. Consequently, the evaluation scope and boundary should be finalised in the early stages of the evaluation project. This decision can be difficult, as it involves balancing consumer needs against evaluation costs.

The Security Target

61 It is very important to get the ST right for the evaluation project. A broad evaluation scope can result in significantly higher evaluation project costs and the potential for a greater number of non-compliances to be identified during the course of the evaluation project.

62 The drafting of the ST requires specific knowledge and experience with the Common Criteria (Ref [3]). Sponsors without sufficient knowledge and experience may find it difficult to prepare the ST for the evaluation project.

63 The ST is further discussed in Section 3.4.3.

Target of Evaluation

64 The term Target of Evaluation (TOE) is central to understanding the scope of the evaluation. The TOE is defined through a set of security functions, and those software and/or hardware elements of an IT product or system that provide that security functionality. In most cases the TOE is a subset of an IT product or system, or a number of IT products.

Assurance Requirements

65 Assurance requirements are organised into pre-defined Evaluation Assurance Levels (EALs) within the Common Criteria (Ref [3]). Assurance levels provide an increasing scale of security confidence, and higher levels of assurance generally come at greater cost. This is due to the more rigorous scrutiny of the TOE and supporting documentation involved (though this does not necessarily involve a larger set of security functionality).

66 The Common Criteria also allows sponsors to define alternative assurance packages for the evaluation of their TOE. Defining a different assurance package requires specific knowledge and experience with the Common Criteria (Ref [3]). Sponsor should contact the MyCB if considering evaluation of a TOE against an alternative assurance package.

67 The assurance level (or assurance package) for the TOE must be decided prior to commencement of the evaluation project as the MySEF must determine the evaluation effort in submitting their proposal for the project to the MyCB.

68 In general the assurance level will affect the level of effort, timeframe, cost of the evaluation and resultant market opportunities.

3.4.3 Identifying Evaluation Evidence

69 The evidence required as input to the evaluation project varies depending on the assurance requirements to be met by the TOE. Sponsors must be prepared to submit the required evidence to the contracted MySEF and the MyCB in accordance with the agreed evaluation schedule.

70 **Note.** The MyCB monitors evaluation project progress against the agreed schedule and delays on the part of the sponsor with the supply of evaluation evidence are sufficient grounds for the MyCB to suspend an evaluation project.

71 Sponsors can use the Part 3 of the Common Criteria (See section 5.1.3) to identify the evaluation evidence that must be provided for an evaluation project. Part 3 of the Common Criteria specifies:

a. **Developer requirements**. The evidence that must be provided by the sponsor;

b. **Content and presentation requirements.** What the evidence provided by the sponsor is required to satisfy; and

c. **Evaluator action requirements.** What must the evaluators do to confirm that the evidence satisfies the Common Criteria.

72 For the evaluation project, the sponsor will be responsible for supplying evaluation evidence of the following types based on the current version of the Common Criteria (Ref [3]):

a. Security Target;

b. Development documentation;

c. Guidance documentation;

d. Lifecycle support documentation; and

e. Test documentation.

Security Target

73 The Security Target (ST) provides the foundation of the evaluation project as it is used to define important elements such as the scope of the evaluation and the security claims against which the product will be evaluated. The ST includes:

a. **An Introduction.** Provides general information about the TOE, identifies the physical and logical scope of the evaluation, and outlines the evaluated configuration.

b. **A Conformance Claim.** Provides a statement of conformance with the Common Criteria (Ref [3]) and any protection profiles.

c. **A Security Problem Definition.** Describes the security aspects of the environment in which the TOE will operate and how it will be used. The TOE security environment includes descriptions of:

i. Assumptions regarding the intended usage of the TOE and its environment

ii. Threats to the TOE that will be countered by TOE security functionality or security measures implemented within its environment

iii. Organisational security policies (OSPs) with which the TOE must comply.

d. **Security Objectives.** High-level objectives that must be satisfied by the TOE or by the environment in which the TOE will operate. These objectives must counter the identified threats and address OSPs and assumptions.

e. **IT Security Requirements.** Describes components (Security Functional Requirements and Security Assurance Requirements) drawn from the Common Criteria (Ref [3]) that will implement the security objectives. These define the set of requirements against which the TOE will be evaluated.

f. **A TOE Summary Specification.** Describes how the TOE meets the IT Security Requirements.

74 Other information may be required in the ST depending upon the assurance level for the TOE and if the sponsor is seeking to extend IT security requirements defined in the Common Criteria. Sponsors should discuss whether additional information will be needed with their contracted MySEF.

Development Documentation

75 The sponsor is required to supply design documentation. The detail and depth required depends on the assurance level to be met by the TOE.

76 The Common Criteria defines a stepwise refinement of the TOE, from the IT security requirements to the actual implementation. Depending on the level of assurance, the sponsor may need to provide information relating to the following:

a. **Functional Specification:** A description of the set of security functions of the TOE and external interfaces.

b. **Security Architecture:** A description of how self protection and non-bypassability of the security functions of the TOE has been achieved.

c. **TOE Design:** A description of how the security functional requirements have been implemented.

d. **Implementation Representation:** The least abstract representation of the TOE. It captures the detailed internal workings of the TOE in terms of source code and/or hardware drawings, as applicable.

e. **Internal Structure of the TOE Security Functions:** Specifications for developing the TOE in a structured manner.

f. **Formal Security Policy Model:** A formal description of the security policy enforced by the TOE.

Guidance Documentation

77 The sponsor is required to provide guidance documentation that covers security preparation and operation of the TOE for all users. In many cases it may be appropriate that guidance is provided in separate documents for preparation and operation of the TOE, or even separate for different user roles as end-users, administrators, application programmers using software or hardware interfaces.

78 The guidance documentation assists consumers with understanding the requirements for secure installation and operation of the TOE and includes:

a. **Preparative guidance:** What must be done to take the TOE as delivered and installs it into its evaluated configuration within the operational environment as described in the ST.

b. **Operational guidance:** What must be done during the operation of the TOE within its operational environment.

Lifecycle Support Documentation

79 Sponsors are required to include information about how discipline and control is maintained during TOE development and maintenance. The types and detail required within lifecycle documentation depends on the assurance level to be met by the TOE. The documentation that may be required includes:

a. **Configuration management:** Describe the characteristics of the Configuration Management (CM) system, and the scope of configuration items that must be managed within the CM system.

b. **Delivery procedures:** Procedures employed for the secure transfer of the finished TOE from the development environment into the responsibility of the user

c. **Development security:** The physical, procedural, personnel and other security measures employed within the development environment for protection of the TOE and its parts.

d. **Flaw Remediation:** The procedures used for the reporting, tracking and remediation of identified security flaws in the TOE.

e. **Lifecycle Definition:** Description of the model used for development and maintenance of the TOE.

f. **Tools and Techniques:** Description of the tools and standards applied for the development of the TOE.

Tests

80 Testing demonstrates that the TOE satisfies the security functional requirements claimed in the ST. The level of assurance to be met by the TOE defines the breadth and depth of testing required for the TOE. Sponsors may be required to provide:

a. **Coverage analysis:** Analyses that demonstrate of the completeness of the functional tests performed by the developer on the TOE.

b. **Depth analysis:** Analysis that demonstrates that functional tests have been completed to a prescribed level in the TOE Design. This may be down to the sub-systems, modules or implementation representation for the TOE.

c. **Functional Test Plans and Results:** Test plans, procedures, expected and actual results of functional testing of the TOE against its security functional requirements claimed in the ST.

d. **The TOE implementation:** The implemented TOE as stated in the ST.

81 In addition, the MySEF will conduct independent testing to verify the evidence provided by the sponsor. As such, sponsors will need to provide material support to the MySEF that might include:

a. Test harnesses, tools and scripts used;

b. Additional hardware, software or firmware used in the functional testing;

c. Specialist test equipment if used by the developer for functional testing; and

d. Technical support personnel to assist with establishment of the test environment.

3.5 Supporting the TOE Evaluation

82 The relationships between the stakeholders for supporting the evaluation are highlighted illustrated in the Figure 5 below.

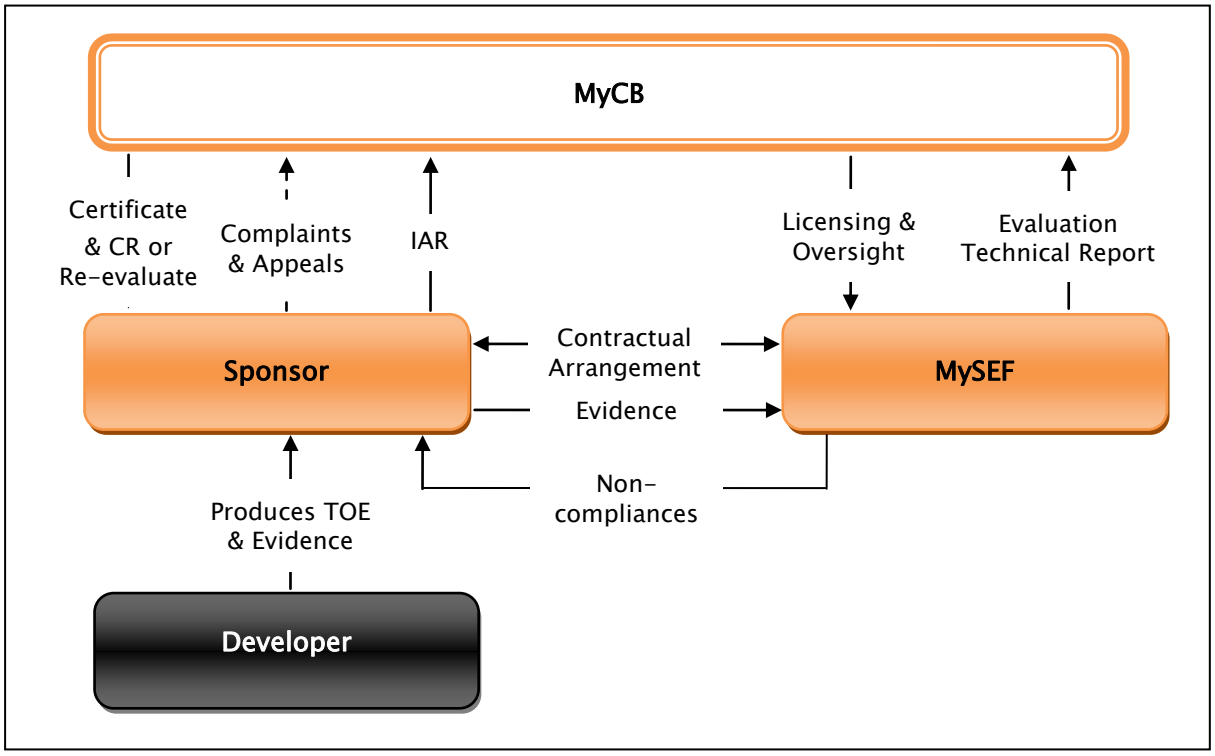

Figure 5: Supporting the TOE Evaluation

83 Sponsors will need to provide a high level of support throughout the process to ensure a successful project outcome. The sponsor will be involved at a number of key milestones during evaluation project including:

a. Acceptance of the evaluation project into the MyCC Scheme;

b. Attendance at the evaluation kick-off meeting;

c. Assisting the MySEF as needed throughout the evaluation project;

d. Resolving non-compliances with the Common Criteria (Ref [3]);

e. Attending evaluation project progress meetings;

f. Assisting with the assessment of the TOE development environment;

g. Reviewing the draft certification report developed by the MyCB; and

h. Attending the evaluation project closedown meeting.

3.5.1 Acceptance of the Evaluation Project

84 The contracted MySEF submits, on behalf of the sponsor, an evaluation project application to the MyCB that includes a number of documents that describe the plan and

scope for the execution of the project. The evaluation application includes the information specified in Section 4.2.4 of the MyCC Scheme Policy (Ref [6]):

85 The MyCB reviews the evaluation project application documentation to determine that:

a. A contract is in place between the sponsor and the MySEF for the evaluation project, and that the sponsor has been made aware of their responsibilities;

b. A reasonable plan for the evaluation is in place;

c. There is no conflict of interest arising in the evaluation project that cannot be effectively managed;

d. The ST forms a sufficient baseline for acceptance of the evaluation project into the MyCC Scheme; and

e. A payment has been included for any certification fees applicable for the evaluation project. Certification fees are published at www.cybersecurity.my/mycc.

86 The MyCB will work with the sponsor and MySEF informally to address any identified deficiencies in the evaluation project application documentation, before reaching their decision. The MyCB will formally advise of the decision to accept or reject an evaluation project application. The rules for rejecting an evaluation application are stated in Section 4.2.4 of the MyCC Scheme Policy (Ref [6]).

87 Where the MyCB rejects an evaluation project application, certification fees that have been paid by the sponsor will be returned.

3.5.2 Evaluation Kick-off Meeting

88 Once an evaluation project has been accepted, the MySEF arranges for the evaluation kick-off meeting to get the project underway.

89 The MySEF is responsible for:

a. Managing the agenda (including distribution prior to the meeting);

b. Inviting the sponsor and the MyCB to attend;

c. Recording minutes of the meeting; and

d. Distributing meeting minutes to attendees.

90 The evaluation kick-off meeting is used to:

a. Ensure that the project is commenced in a controlled manner and that all stakeholders are aware of their roles and responsibilities.

b. Provides all parties with an opportunity to discuss the upcoming evaluation project.

c. Provide an opportunity for the MyCB to discuss the rules and requirements for the project

d. Confirm the agreed schedule and required deliverables.

e. Provide an opportunity for the sponsor to raise areas of concern or ask questions of the MyCB or MySEF about the evaluation project.

91 Minutes of the Evaluation Kick-off Meeting should be provided by the MySEF to the sponsor within **five (5)** business days of the conduct of the meeting, and agreed within **ten (10)** business days of the conduct of the meeting.

3.5.3 Assisting the MySEF

92 The sponsor must provide assistance to the MySEF to minimise potential for slippage of the agreed schedule.

93 **Note.** The MyCB monitors evaluation project progress against the agreed schedule and a failure to provide adequate assistance on the part of the sponsor are sufficient grounds for the MyCB to suspend an evaluation project.

94 Evaluation project progress depends on the submission of evaluation deliverables in accordance with the agreed schedule and the timely resolution of non-compliances identified by the evaluators.

95 Sponsors should be aware that IT security evaluation is an iterative process and it is likely that non-compliances with the IT security evaluation criteria will be identified during the evaluation project. It is the responsibility of the sponsor, and not the MySEF, to resolve identified non-compliances in a timely manner so as to not impact the agreed evaluation project schedule.

Changing the version of the TOE

96 The MySEF and the MyCB must be consulted where a sponsor intends to change the version of the TOE that has been accepted into the MyCC Scheme. Changes to the version of the TOE can incur significant rework by the MySEF and hence may increase the costs to the sponsor for the evaluation project.

Testing Support

97 Additional support is usually required for evaluator testing in the evaluation project. Testing occurs late in the evaluation project and is usually conducted at the MySEF, but some or all testing may also occur at the development site facilities. Evaluators may need assistance with the installation and configuration of the product or system, and delivery of specialist test equipment may be required. Sponsors should work with the contracted MySEF to ensure that support needs are determined well in advance to avoid delays in the evaluation project.

Product Training

98 Sponsors may be requested to provide product or system specific training. Training can assist evaluators and/or certifiers with familiarisation on the installation and use of the product or system and can hasten the evaluation project. To maximise the benefits to all stakeholders, this training should be conducted in the early stages of the evaluation process.

3.5.4 Resolving Non-compliances

99 The evaluators will discover non-compliances against the Common Criteria (Ref [3]) for the TOE and/or its evaluation evidence during an evaluation project.

100 Non-compliances are recorded as an Evaluation Observation Report (EOR). EORs will be classified as having either a minor or major impact on security for the TOE. The objective of an EOR is to ensure that the sponsor, the MyCB and the MySEF have a formal record of non-compliances so that appropriate action can be taken.

101 **Note.** The MySEF cannot propose or conduct specific implementation activities to resolve non-compliances. The sponsor must determine and implement the corrections to the evaluation evidence to the satisfaction of the evaluators and certifiers to resolve non-compliances.

102 Very rarely, a minor non-compliance may be passed to the MyCB for resolution during the certification process. In these cases, the sponsor works to resolve the non-compliance with the certifier before the certification process can be completed.

3.5.5 Project Progress Meetings

103 Project progress meetings will be held as needed throughout the evaluation project and are initiated by either the MySEF or the MyCB. If a sponsor requires a project progress meeting, the contracted MySEF is responsible for initiating the meeting on their behalf. These meetings provide an opportunity for all parties to discuss the progress of the evaluation project, scheduling and/or management of the project.

104 The MySEF is responsible for:

a. Managing the agenda (including distribution prior to the meeting);

b. Inviting the sponsor and the MyCB to attend;

c. Recording minutes of the meeting; and

d. Distributing meeting minutes to attendees.

105 The sponsor should receive draft minutes of the evaluation project meeting within **five (5)** business days of the conduct of the meeting and is required to provide comments or confirmation of the minutes within **five (5)** business days of receipt.

3.5.6 Assisting Development Site Visits

106 Depending upon the Security Assurance Requirements to be met by a TOE, a visit by the evaluators to the TOE development site(s) may be required. Development site visits (DSV) are used by evaluators to gain assurance in aspects of TOE lifecycle support including:

a. Development site security;

b. Configuration management; and

c. Delivery procedures.

107 In some circumstances, the evaluators may be able to gain assurance by methods other than conducting a DSV. The evaluators are required to justify such an approach in their Evaluation Project Proposal to the satisfaction of the MyCB. If a DSV is required, a minimum of two evaluators must attend. The MyCB has the option of sending one member of the certification team to the DSV paid for by the sponsor. The MyCB is

obliged to inform the sponsor when accepting their evaluation project into the MyCC scheme if this option will be exercised.

108 The effort and duration of the site visit depends on:

a. The level of assurance to be met by the TOE; and

b. The number and distribution of TOE development sites.

109 The MySEF is required to develop and submit a plan to the MyCB for the DSV. When developing this plan, the MySEF consults with the sponsor and the MyCB to ensure that the dates proposed for the DSV are suitable to all stakeholders. It is essential that the development site is made available to the MySEF when requested to avoid delays in the evaluation project.

3.5.7 Reviewing the Draft Certification Report

110 The MySEF provides a document to the MyCB at the completion of all evaluation activities providing the results of the evaluation project. This document is called and Evaluation Technical Report (ETR) from which the MyCB will produce the Certification Report (CR). The ETR is internal to the MyCC Scheme and not for release to the sponsor (or any other party) as it may contain sensitive information on the tools and techniques used for evaluator testing of the TOE. A sponsor may request a sanitised version of the ETR from the contracted MySEF. The MySEF is required to submit the sanitised version of the ETR to the MyCB for approval prior to releasing it to the sponsor. Sanitisation typically involves removal all information related to evaluator testing conducted on the TOE.

111 The CR provides:

a. A statement of the TOE conformance with its Security Target;

b. Confirmation that the assurance requirements claimed in the evaluation have been met;

c. Confirmation that the evaluation has been conducted in accordance with the MyCC Scheme rules and that the conclusions drawn from the evaluation are consistent with the facts presented;

d. A listing of any residual vulnerabilities in the TOE, and any recommended countermeasures; and

e. Additional guidance that the MyCB considers necessary to include on the secure delivery, installation, configuration and operation of the TOE.

112 Sponsors are provided **five (5)** business days to review and submit feedback to the MyCB. Comments received by the MyCB are reviewed and may be incorporated into the final CR. The CR is a public document and will not contain sensitive information about the product, system and/or the evaluation process.

3.5.8 Project Closure Meeting

113 The objectives of the project closure meeting are:

a. To close the evaluation project in a controlled manner;

b. Confirm disposal and archive arrangements for evaluation evidence related to the evaluation project;

c. Obtain feedback on customer experience with the MyCC Scheme, the MyCB and the MySEF;

d. Discuss lessons learned and opportunities for improvement; and

e. Discuss MyCC Scheme certificate maintenance services.

114 The MySEF is responsible for:

a. Managing the agenda (including distribution prior to the meeting);

b. Inviting the sponsor and the MyCB to attend;

c. Recording minutes of the meeting; and

d. Distributing meeting minutes to attendees.

115 Sponsors should receive draft meeting minutes within **five (5)** business days on the conduct of the meeting, and have a further **five (5)** business days to provide comments on the draft minutes.

3.6 Maintaining TOE Assurance

116 The relationships between the stakeholders during assurance maintenance are highlighted illustrated in the Figure 6 below. Note that “re-evaluation” is not represented in this figure as it is treated as a new evaluation (though with significant re-use). The relationships in an evaluation are defined in Figure 4 and Figure 5.

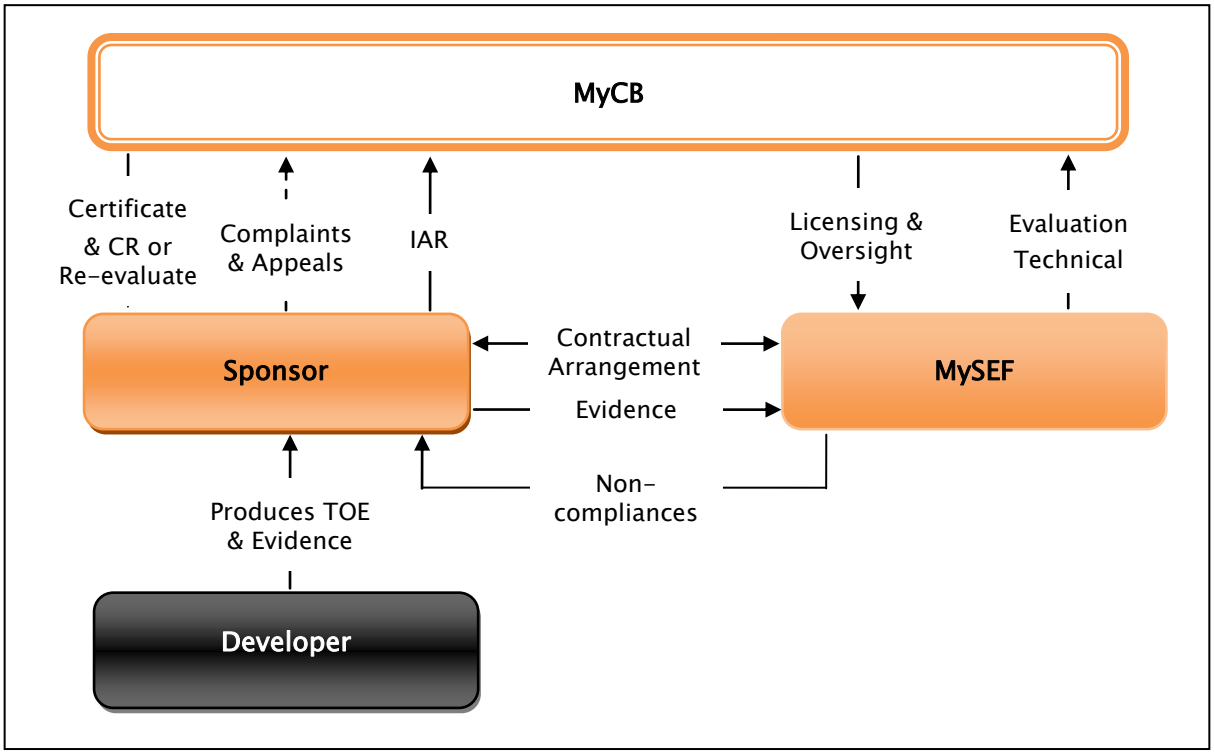

Figure 6: Assurance Maintenance

117 Developers have a need to continuously improve their IT products and systems. This may be to add new functionality, improve performance of existing functionality, correct errors or fix discovered security vulnerabilities.

118 When a developer updates a certified product or system outside of the MyCC Scheme, the resultant product or system is no longer considered to be in its evaluated configuration and unable to claim any security certification. Consumers of the product or system may be left uncertain as to whether to move to the updated version or stay with the certified version.

119 For sponsors, the cost of the original evaluation and certification may not be justifiable where a product or system changes shortly after completing the evaluation project.

120 To balance the requirements of sponsors, developers and consumers, a pragmatic and cost-effective approach to maintaining assurance in a certified product or system has been implemented within the MyCC Scheme. This approach is conformant with the Common Criteria Recognition Arrangement Approach to Assurance Continuity (Ref [5]). This means that changes to products and systems that have been certified in the MyCC Scheme may be recognised across all countries that are part of the CCRA.

121 Maintenance of Assurance incorporates two main activities:

a. **Maintenance.** The process of reviewing and accepting 'minor' modifications to a certified product or system that do not impact on its security-enforcing functionality.

b. **Re-evaluation.** The process undertaken where a change to a certified product or system is considered 'major'. Re-evaluation aims to make maximum reuse of

previous evaluation results, with the goal of making the process as cost-effective and efficient as possible.

122 Unlike an evaluation project, the maintenance of assurance occurs between the MyCB and the sponsor. **Note.** The MyCB charges fees based on the number of hours spent by MyCB resources assigned to reviewing changes to a certified TOE.

3.6.1 Entering into Maintenance

123 A product or system is required to have been certified (a certified TOE) by the MyCC Scheme before it can enter into the maintenance of assurance process. To enter into maintenance, the MyCC Scheme requires sponsors to submit a letter of intent to participate in maintenance of assurance to the MyCB.

124 **Note.** The MyCB allows **thirty (30)** business days following certification of a product or system for a sponsor to lodge their letter of intent to participate in maintenance of assurance.

125 Following MyCB acceptance into maintenance of assurance, the MyCB will assign a certifier to act as the technical representative for all maintenance activities for the certified TOE. The first activity for the MyCB certifier will be to arrange an initial meeting with the sponsor and developer. The objectives of this initial meeting are:

a. Introduce the MyCB certifier that will be the technical point of contact for maintenance of assurance activities;

b. Provide the formal notification of acceptance of the certified TOE into the maintenance of assurance program;

c. Provide a general overview of the maintenance of assurance process within the MyCC Scheme;

d. Confirm of fees and charges associated with the maintenance of assurance process; and

e. Provide a general overview of the complaints, disputes and appeals processes and the relevant provisions of the MyCC Scheme Policy (Ref [6]).

126 The MyCB certifier assigned is responsible for:

a. Scheduling and organising the Initial Meeting with the customer (sponsor/developer);

b. Preparing and circulating the agenda at least **two (2)** business days before the meeting;

c. Confirming attendees; and

d. Conducting the meeting.

3.6.2 Reporting Changes to the Certified TOE

127 The sponsor is required to submit an Impact Assessment Report (IAR) for changes to a certified TOE. Details on the information required in an IAR can be found in the CCRA requirements for assurance continuity (Ref. [5]). The MyCB aims to acknowledge receipt of an IAR within **two (2)** business days.

Accepting Maintained Versions

128 Maintenance offers sponsors the opportunity to have the latest update of their certified TOE recognised with minimal effort and/or expenditure. Accepting changes to a certified TOE under maintenance requires that the MyCB assessment of those changes is minor as defined by the CCRA requirements for assurance continuity (Ref. [5]).

129 The MyCB aims to complete it assessment of changes within **five (5)** business days of receipt of an IAR.

130 Once the MyCB has determined that the update or modification is minor, a maintenance addendum is issued to the sponsor and the MyCPR is updated to reflect the maintenance activities.

Re-evaluation

131 A re-evaluation is the outcome where the MyCB determines that the changes to a certified TOE have major impact on the assurance baseline, and the sponsor chooses to continue with maintaining assurance. Re-evaluation is performed in context of the earlier evaluation, reusing any results from the assurance baseline that still apply. The sponsor must engage a MySEF for the re-evaluation project.

132 Where the MyCB assesses the change as major in accordance with the CCRA requirements for assurance continuity (Ref. [5]) the sponsor will be informed formally in writing of the outcome. The sponsor then has **twenty (20)** business days to inform the MyCB that they are considering re-evaluation.

133 If the sponsor informs the MyCB that they are considering re-evaluation, the MyCB will wait for notification that the sponsor has contracted with a MySEF for the re-evaluation project and an invitation from the MySEF to attend a re-evaluation planning meeting.

134 The re-evaluation project will aim to reuse a significant portion of the evaluation results of the original certified TOE. The amount of possible reuse depends on the number and scope of the changes to the security functionality within the original certified TOE. Once the level of reuse has been determined, an evaluation project is commenced (see section 3.5 for sponsor support requirements). The sponsor may then continue the new certified TOE under maintenance of assurance.

3.7 Use of Marks and Notifications

3.7.1 Sponsor Marketing

135 Sponsors may market that they have a product or system undergoing evaluation in the MyCC Scheme once it has been formally accepted by the MyCB provided that:

a. The marketing clearly identifies only the version of the product or system that is undergoing evaluation and no others.

136 The sponsor may not use any MyCC Scheme or CCRA (Ref [1]) logo until certification has been achieved.

137 Once accepted into the CCRA as a certificate authorising participant, certificates issued by the MyCC Scheme will bear the following marks.

Figure 7: CC Certification Mark

Figure 8: MyCC Certification Mark

138 Upon receipt of a MyCC Scheme CC certificate, sponsors may use the marks in Figure 7 and Figure 8 in conjunction with advertising, marketing and sales of the product for which the certificate is issued.

139 Sponsors should seek approval from the MyCB before releasing any material that refers to the MyCC Scheme, MyCB or CyberSecurity Malaysia prior to its release.

3.7.2 Notifications

140 Sponsors should inform the MyCB of planned future releases of the TOE. Sponsors interested in an enhanced return on investment are strongly encouraged to participate in maintenance of assurance activities as part of their product development roadmap.

141 Sponsors should notify the MyCB when:

a. Their contact details change to ensure that the MyCPR is current;

b. There is a firm intent to cease sales and/or technical support of their certified TOE; and/or

c. They become aware of an exploitable vulnerability in their certified TOE.

142 Sponsors must respond in a timely manner when requested by the MyCB to provide product release, availability and vulnerability information.

3.7.3 Misuse of Certification Marks

143 Sponsors and Developers may not use the marks in Figure 7 and Figure 8 in anyway other than those described in this section or explicitly authorised by the MyCC Scheme.

144 The MyCB will monitor the use of the CC Certification Mark and the MyCC Certification Mark. If a sponsor or developer is found to be misusing either of the marks, the MyCB will take one or more of the following actions:

a. Notify the infringing party of the issue; and/or

b. Withdraw the certificate(s) that is associated with the infringement.

3.8 Disputes, Complaints and Appeals

145 Disputes, Complaints and Appeals are handled by the MyCB in accordance with the MyCC Scheme policy. The procedure for making a complaint is detailed on www.cybersecurity.my/mycc.

4 Guidance for Consumers

4.1 Overview

146 This section provides guidance for consumers of MyCC Scheme certified products and systems on their benefits, procurement and secure usage within their IT environments.

147 This guidance is provided in the following sections:

a. **Benefits of using certified products and systems:** An overview of the benefits arising from use of certified products and systems.

b. **Selection:** Guidance on making an informed decision when selecting evaluated products and systems.

c. **Acquisition:** Guidance in relation to the acquisition and delivery of an evaluated product or system.

d. **Preparation:** Guidance for initialising the product or system into its evaluated configuration.

e. **Operation:** Guidance for using and administering an evaluated product and systems in a secure manner.

4.2 Benefits of using Certified Products and Systems

148 Information managed by ICT products is a critical business resource supporting the mission of an organisation. Individuals also have a reasonable expectation that their personal information managed by ICT products remains confidential, is available to them as needed, and is not modified. ICT products should deliver their functionality while exercising proper control over the information thereby ensuring it is protected against security threats.

149 Consumers of ICT products may have limited knowledge, expertise or resources available to determine whether their confidence in the security of their ICT products is appropriate. Further, they may not wish to rely solely on the assertions of the developers when selecting ICT products to meet their needs. Instead, consumers may benefit from independent security evaluation that provides a degree of assurance that an ICT product correctly performs its functions, while reducing the likelihood of security flaws being present.

150 In summary, products and systems that have undergone IT security evaluation and certification provide grounds for confidence that they:

a. Will meet consumer security needs;

b. Function as specified;

c. Have adequate guidance;

d. Can be operated securely;

e. Have been built correctly;

f. Have been delivered as requested;

g. Has been thoroughly tested; and

h. Have reduced the potential for exploitable vulnerabilities in their implementation.

4.3 Selection

151 Two certified products or systems may appear similar in functionality; although the actual evaluated security functionality may be very different. In order to make an informed decision before purchasing a certified product, consumers should review the following important evaluation documents:

a. The Security Target (ST); and

b. The Certification Report (CR).

4.3.1 Reviewing the ST

152 The ST provides important information about the scope of the evaluation, the intended environment in which the product or system is to be operated and the set of security functional and assurance requirements against which it was evaluated.

153 Consumers need to be aware of the IT security evaluation term 'Target of Evaluation (TOE)' (see Section 3.4.2). The TOE provides the boundary and scope of the evaluation and, in most cases, is a subset of an IT product or system, or a number of IT products.

154 Sponsors are able to elect which security functions are included within the scope of the evaluation. This means that two similar IT products or systems may have completely different TOEs and evaluated functionality. Consumers should take time to understand the evaluation scope when selecting a certified product or system.

155 The ST is the defining document for understanding evaluation scope. The ST introduction should provide a description of the TOE in natural language summarising the security features included. Consumers should read the section carefully, cross referencing with later sections in the ST, as it may describe supporting functionality that is not included in the scope of the evaluation.

156 The security problem definition of an ST provides important consumer information on the specific characteristics of the environment in which the TOE is intended to operate. Consumers should review this section to ensure that characteristics of the intended environment align with their operational needs and the security problem that they are trying to solve.

157 The TOE's intended environment is described by:

a. Assumptions regarding the intended usage of the TOE and its environment;

b. Threats to the TOE that will be countered by TOE security functionality or security measures implemented within its environment; and

c. Organisational security policies (OSPs) with which the TOE must comply.

158 The security objectives stated in an ST for a certified product or system have been determined by evaluation to be upheld by the TOE within its intended operating environment.

159 The security requirements stated in an ST provide the set of security functional and assurance requirements against which the TOE was evaluated. Security functional requirements (SFRs) provide the set of security functions that the TOE implements. These statements are made using a semiformal notation that has been drawn from Common Criteria (Ref [3]). The security assurance requirements (SARs) identify what was satisfied to gain assurance that the security functional requirements have been met by the certified TOE. The set of SFRs and SARs provides the foundation for direct comparison between two similar IT products.

4.3.2 Reviewing the CR

160 The CR provides:

a. A statement of the TOE conformance with its Security Target;

b. Confirmation that the assurance requirements claimed in the evaluation have been met;

c. Confirmation that the evaluation has been conducted in accordance with the MyCC Scheme rules and that the conclusions drawn from the evaluation are consistent with the facts presented;

d. A listing of any residual vulnerabilities in the TOE, and any recommended countermeasures; and

e. Additional guidance that the MyCB considers necessary to include on the secure delivery, installation, configuration and operation of the TOE.

161 Consumers should read the CR to ensure that any additional recommendations that are not documented in the ST are considered in their selection of a certified product or system.

162 A MyCC Scheme CR is conformant with the CCRA requirements for a CR (Annex I of Ref [1]).

4.4 Acquisition

163 Once the decision to acquire a certified product or system has been made, the consumer should request the evaluated version and supporting documentation from the sponsor.

164 For all Common Criteria evaluations at EAL2 and above, the secure delivery procedures employed for the certified product or system have been evaluated. These procedures provide confidence that the product or system received by the consumer is the certified product or system and has not been compromised in transit.

165 Consumers should request the secure delivery procedures from the sponsor prior to acquisition and then ensure that the procedures have been followed for the delivered certified product or system.

4.5 Preparation

166 Certified products and systems should be delivered with guidance on installing and configuring the TOE so that consumers may install the product in its evaluated configuration. This documentation is known as the preparative procedures.

167 If consumers elect to use a product or system outside of its evaluated configuration, no statement can be made as to the assurance in its security functions. A certification only provides assurance in the security functions when the TOE is configured in accordance with the evaluation configuration as defined in the Security Target of the certified product and associated guidance

168 Consumers are reminded that assurance is a measure of confidence in the security functions of the product or system and this does not reduce the consumer's responsibility to protect their information.

169 A certified product or system is considered outside of its evaluated configuration if:

a. Security functionality is utilised that was not within the scope of the evaluation;

b. Security functionality is used that was within scope but has not been configured in accordance with the preparative procedures supplied by the sponsor;

c. Patches or product upgrades are applied; and/or

d. The operational environment in which the certified product or system TOE is being utilised does not comply with the security environment described within the ST.

4.6 Operation

170 The CC requires that the sponsor provide guidance for secure operation of a certified product or system. It is recommended that consumers ensure that acquired certified products and systems are supplied with operational documentation covering all user types.

171 Operational guidance helps ensure that users understand the environmental constraints of the TOE, how to perform their role and how to correctly manage and use those security functions relevant to their role.

5 Overview of Common Criteria

172 The IT security evaluation criteria used by the MyCC Scheme for the delivery of certification and evaluation services is the Common Criteria (Ref [3]) (CC). The CC was created to harmonise criteria produced by a number of nations, including the United Kingdom, Canada and the United States, into a single set of common criteria. The CC is now recognised as an ISO (International Organization for Standardization) standard and regarded as the international benchmark for IT security evaluation criteria.

173 The current version of the CC used within the MyCC Scheme is identified in Annex A of the MyCC Scheme Policy (Ref [6]) and Annex A of this manual.

5.1 Common Criteria Structure

174 The CC is comprised of three parts as illustrated in Figure 9 below.

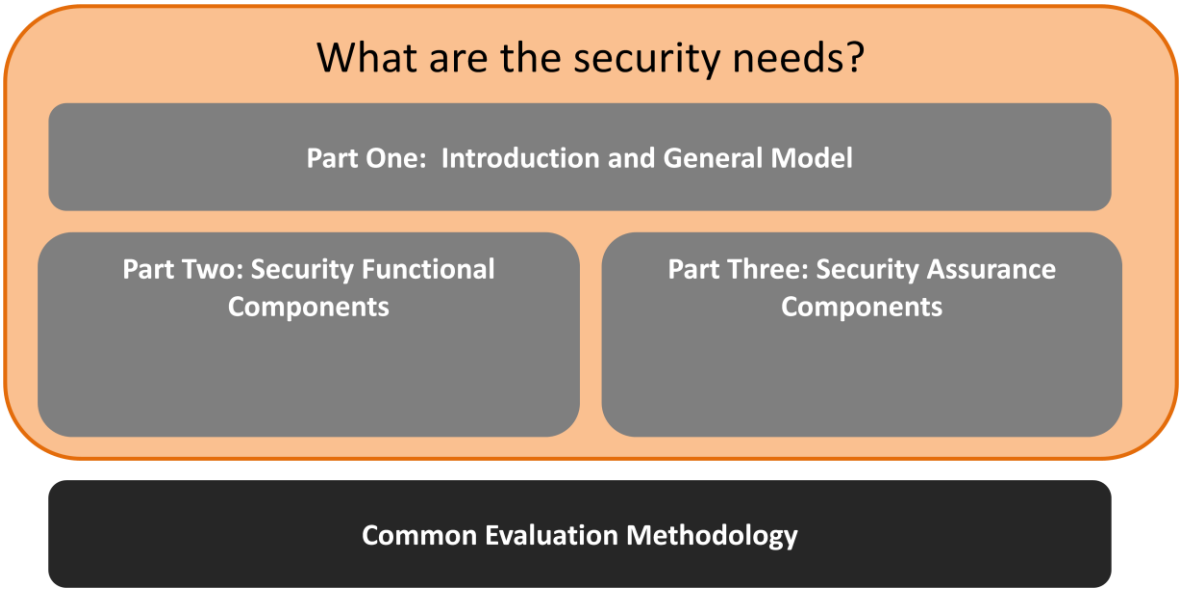

Figure 9: Structure of the CC

5.1.1 Part 1 Introduction and General Model

175 Defines general concepts and principles of IT security evaluation and presents the paradigm of evaluation.

5.1.2 Part 2: Security Functional Components

176 Provides a catalogue of functional requirements for sponsors to utilise in defining the IT security functions. These requirements are considered claims that the sponsor is making about product or system IT security capabilities.

177 These security functional requirements fall into logical groupings described in Table 2 below.

Table 2: Security Functional Requirements Groupings

Functional Grouping	Description
Audit	Requirements for recognising, recording, storing, and analysing information related to security relevant activities.
Communication	Requirements for assuring the identity of a party participating in a data exchange.
Cryptographic support	Requirements for the management and use of cryptographic keys.
User data protection	Requirements for the protection of user data.
Identification and authentication	Requirements associated with establishing and verifying a user's claimed identity.
Security management	Requirements for the management of security functions such as the management of security attribute.
Privacy	Requirements for providing a user with protection against the discovery and misuse of identity by other users.
Protection of the TSF	Requirements for protecting the integrity and management of mechanisms providing the TOE's security functionality.
Resource utilisation	Requirements that support the availability of required resources such as processing capability and/or storage capacity.
TOE access	Requirements for controlling the establishment of a user's session.
Trusted path/channels	Requirements for a trusted communication path between users and the TOE and for a trusted communication channel between the TOE and other trusted IT products.

5.1.3 Part 3: Security Assurance Components

178 Provides a catalogue of assurance components, which are the requirements that the TOE will be evaluated against. Part 3 also defines Evaluation Assurance Levels (EALs) that provide a predefined scale for benchmarking assurance for TOEs.

179 These EALs are described in Table 3 below.

Table 3: Evaluation Assurance Levels

EAL	Description
EAL1 – functionally tested	Applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. Of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.
EAL2 – structurally tested	Applicable in those circumstances where developers or consumers require a low to moderate level of independently assured security in the absence of ready availability of the complete development record.
EAL3 – methodically tested and checked	Applicable in those circumstances where developers or consumers require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.
EAL4 – methodically designed, tested and reviewed	Applicable in those circumstances where developers or consumers require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs
EAL5 – semi-formally designed and tested	Applicable in those circumstances where developers or consumers require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.
EAL6 – semi-formally verified design and tested	Applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.
EAL7 – formally verified design and tested	Applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

Augmentation

180 In addition to selecting a CC EAL, sponsors may:

a. Augment the level of assurance for a TOE. Augmenting assurance involves selecting additional security assurance requirements from the CC Part 3, that are not prerequisites for the selected CC EAL; or

b. Define new assurance packages from the CC components.

181 An augmented EAL is denoted on certificates by using an addition sign after the EAL, for example, 'EAL2+'. In the case of augmented assurance, details of the additional assurance provided will be outlined within the Certification Report (CR) and on the certificate for the TOE.

5.1.4 Common Evaluation Methodology

182 The CC is also supported by a methodology that provides evaluators with guidance on how to apply the criteria. The CC methodology is known as the Common Methodology for Information Technology Security Evaluation (CEM).

Annex A Reference Material

A.1 References

[1] Arrangement on the recognition of Common Criteria Certificates in the field of Information Technology Security, July 2014.

[2] 9th Malaysian Plan (2006-2010), *Chapter Five – Mainstreaming Information and Communications Technology*, Paragraphs 5.74, 5.75 and 5.76.

[3] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[4] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

[5] Assurance Continuity, CCRA Requirements, Version 2.1, June 2012.

[6] MyCC Scheme Policy (MyCC_P1), CyberSecurity Malaysia, v1d, February 2016.

A.2 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
CM	Configuration Management
CR	Certification Report
DSV	Development Site Visit
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
IAR	Impact Analysis Report
ICT	Information and Communications Technology
ISCB	Information Security Certification Body
ISO	International Standards Organisation
IT	Information Technology
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body

Acronym	Expanded Term
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
TOE	Target of Evaluation

A.3 Glossary of Terms

Table 5: Glossary of Terms

Term	Definition and Source
Certificate	The official representation from the Certification Body of the certification of a specific version of a product to the Common Criteria.
Certification Body (MyCB)	An organisation responsible for carrying out certification and for overseeing the day-today operation of an Evaluation and Certification Scheme.
Consumer	The organisation that uses the certified product within their infrastructure.
Certification Report	Final report issued by the Certification Body providing certification details of an evaluation and providing guidance to consumers.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme.
Evaluation and Certification Scheme (MyCC Scheme)	The systematic organisation of the functions of evaluation and certification under the authority of a certification body in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved.
Evaluation Technical Report	Final report produced by the Security Evaluation Facility documenting the conduct and results of an evaluation. The ETR is submitted to the Certification Body.

Term	Definition and Source
Information Security Certification Body	A department within CyberSecurity Malaysia that manages and provides certification services focusing on the security against international standard and guidelines.
Lead Certifier	The Certifier responsible for managing a specific certification task.
Lead Evaluator	The Evaluator responsible for managing the technical aspects of a specific evaluation task.
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
Protection Profile	Document that defines a statement of security requirements for a specific product or system type. Generally specified by a user community to convey requirements. Differs from a Security Target.
Security Evaluation Facility (MySEF)	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Security Target	Document that defines the scope of an evaluation and the security claims against which a product or system will be evaluated. Generally specified by a developer to specify security claims. May claim conformance to a Protection Profile.
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.
Target of Evaluation	Defined by the Security Target. The TOE refers to the specific parts of a product or system that are within the scope of evaluation.

--- END OF DOCUMENT ---