

# **How do you ensure evaluators are competent?**

[ICCC 2010 Paper Submission]

Zarina Musa

Evaluator

CyberSecurity Malaysia MySEF, Kuala Lumpur, Malaysia

## ***Abstract***

Ensuring the evaluators in a security evaluation facility are competent in their job is not a simple task. There is no one sure method of giving us this assurance. This is more true for a newly set-up evaluation facility with new evaluators. CyberSecurity Malaysia MySEF (Malaysian Evaluation Facility) has been set-up just about 2 years ago, and we are currently looking at increasing number of products coming in for evaluation. How do we ensure that our evaluators have the necessary skills within an acceptable timeframe? Training a large number of new evaluators requires proper planning. We will share our approach and experience, and hopefully this paper will encourage more discussions for the benefit of all.

## **Objective**

The objective of this paper is to impart our experiences in ensuring that our evaluators are competent and have the necessary skills to perform Common Criteria evaluations.

## **Introduction**

I am representing CyberSecurity Malaysia MySEF, and let me first give an introduction on how our evaluation facility came into existence.

The first project of Ninth Malaysian Plan for CyberSecurity Malaysia (formerly NISER) established the requirements for the Malaysian Common Criteria (MyCC) Scheme. The aims are to increase Malaysian competitiveness in quality assurance of information security using the CC standard, and to build consumer confidence in Malaysian information security products and systems. Security Assurance, a department within CyberSecurity Malaysia, has responsibility for providing expert services in ICT security product and system evaluation based on the CC (MS-ISO/IEC 15408). Its objectives are to promote a safe and reliable computing environment

through the provision of assured ICT security products. Evaluation services are necessary to provide confidence in the security capabilities of ICT products and systems in defending against ICT threats.

In 2007, CyberSecurity Malaysia commenced a project to establish the MyCC scheme beginning with the development of the scheme strategy and its associated implementation plan. In response, CyberSecurity Malaysia MySEF was established, and it was the one and only Common Criteria evaluation facility in Malaysia.

Once established, we started on a few pilot projects and then proceed to trial evaluation projects as we aim to fulfill the requirements to be an authorizing member of the CCRA. As we are looking at increasing number of products coming in for evaluation, a large number of new evaluators are hired. Who are they? They are IT and engineering graduates, and some of our requirements include good performers in college, good attitude, high achievers and the most important thing is that they must be interested in becoming an evaluator. They also must have a basic level of knowledge in IT security. Some of them are fresh graduates and have no working experience. Almost all of them do not have any exposure and have not attended any formal training on Common Criteria.

Now we've come to the main point of this paper, how do we ensure that these new evaluators are competent in performing Common Criteria evaluations.

For a newly set-up evaluation facility, and with a number of new evaluators in our hands, we have to ensure that they have the necessary skills within an acceptable time-frame. Proper planning is needed. The purpose of this paper is to share what we have been doing, our approach and experience.

We feel that the first thing we need to ensure is their knowledge of IT security. So, the first thing that we do is conduct internal trainings on various subjects related to ICT, ICT security and specific product trainings in order to provide fundamental knowledge and build the competency level of MySEF new evaluators, and also to ensure their correct and common understanding of the subject. We provide basic (as a refresher) and intermediate level trainings. We've conducted a series of trainings such as cryptography, VPN(IPSEC), network security, access control, Unix security, web application security, biometrics and wireless. After we've covered the basics, we

also send the evaluators to more advanced and specialized trainings, which is in line with ISO 17025 requirement which requires that continuous training must be provided to maintain and increase competency.

We also conduct regular Knowledge Sharing sessions among us. This is to ensure that the evaluators are aware of new technologies and are up-to-date with current aspects of the IT security. The sessions are also used to refresh the evaluator's understanding of the main principles of IT security. Evaluators who went for formal trainings to increase competency is also required to conduct knowledge sharing to other evaluators in MySEF within one month of training completion. This is to ensure that knowledge gained is being shared with others. The frequency of these sessions depends on the availability of the presenters and evaluators, but we aim to conduct it once in every two weeks.

We feel that we need to continuously update and also refresh ourselves on penetration testing techniques. So, we also conduct demos on penetration testing among ourselves. These are hands-on classes, so all evaluators can be involved and can try executing the steps themselves. These classes are conducted weekly, but depending on the availability of the presenter and evaluators.

Next, we go on to the strategies for gaining competency in MyCC Scheme (Malaysian Common Criteria Scheme), certification and evaluation functions. This training strategy uses MyCC Scheme expertise to provide up to a working level of competency in the operation of the MyCC Scheme and the Common Criteria evaluation and certification.

All our new evaluators must attend the formal MyCC scheme training conducted by senior personnels from the MyCB and MySEF. These trainings should deliver both basic and intermediate level of competency to MySEF Evaluators. The modules involved provide a basic competency in IT security evaluations and the MyCC Scheme, provide a basic competency in Security Targets, Protection Profiles, functionality and assurance requirements (supported by a case study) and provide a working level competency in Security Targets and Protection Profiles, assurance components. Competency will be verified by question and answer sessions with the students. A MyCC Scheme Common Criteria examination will be administered to the students, and passing it demonstrates their mastery of the subject matter.

Apart from this formal training, we also conduct a one week hands-on evaluation training. We prepared exercises for ASE, ADV, AGD, ALC, ATE evaluation phases and divided the class into several groups. Each group will work on one evaluation phase and discussions and presentations will be held which involve all participants in the class.

Our next strategy for ensuring competency is implementing a mentor-mentee program. This program is necessary for new evaluators. Each new evaluator will be attached to a senior MySEF evaluator who will become his/her mentor. This is a one-to-one or one-to-two kind instead of one-to-many training. This personal training enables more focused and flexible environment. Pace is depending on mentor, as long as it is within the allocated timeframe.

This training program consists of hands-on evaluation exercise. The exercise will be done on selected Target of Evaluation (TOE) which will be evaluated for EAL1+ assurance level.

Evaluations will be done using Part 1, Part 2 and Part 3 of Common Criteria for Information Technology Security Evaluation MS-ISO/IEC 15408 and Common Methodology for Information Technology Security Evaluation MS-ISO/IEC 18045 and in conformance with MyCC Scheme Policy, under the guidance of each assigned mentor.

Mentor's responsibilities are to provide their mentees with relevant evidence documents and workbooks at the beginning of each module, coach and provide guidance to their mentees during the evaluation exercises, ensure that their mentee completes the assigned module according to schedule, perform a peer review on the completed workbooks, discuss the findings with their mentee and share the correct evaluation verdict and assess mentee's work performance and efficiency level by filling in Section B of the Common Criteria Training Evaluation Form. Whereas, mentee's responsibilities are to perform evaluation exercises and complete workbook and Evaluator Notes, complete the assigned module according to schedule, discuss the findings with their mentor and share the correct evaluation verdict and evaluate their understanding of the training by filling in Section A of the Common Criteria Training Evaluation Form. Mentors will be provided with an answer scheme, to guide them even though it is up to them how they choose to elaborate on the answers.

There will be 6 modules involved in this program and they are required to be completed as an exercise before the mentees can conduct any actual evaluation works. At the beginning of the

program, a briefing for the mentees will be given by a senior MySEF personnel, which gives an overview of the whole training program such as the modules involved and the schedule. The modules cover ASE evaluation (Security Target), AGD evaluation (Guidance Documents), ADV evaluation (Development), ALC evaluation (Life-Cycle Support), ATE evaluation (Tests) and AVA evaluation (Vulnerability Assessment). We have a tentative schedule which specifies the allocated timeframe for each module and mentors are responsible to ensure the completion is according to schedule. After the briefing, mentors are to provide their mentees with EOR and Evaluator Notes template. In addition, mentors will provide relevant evidence documents and workbooks at the beginning of each module. Before the start of the ATE evaluation (Tests) and AVA evaluation (Vulnerability Assessment), a briefing will be done by senior MySEF personnel. This is to ensure the mentees have sufficient knowledge and understanding in order to perform ATE and AVA evaluations. This briefing will cover the following topics :

- a. Overview of ATE and AVA Evaluation
- b. Drafting a Test Plan for Functional Testing (ATE\_FUN.1)
- c. Mapping between Test Script with TSFI in Functional Specification document (ATE\_COV.1)
- d. Drafting a Test Plan for Independent Testing (ATE\_IND.2)
- e. Drafting a Test Plan for AVA\_VAN.2 Testing
- f. Calculating Attack Potential
- g. Creating environment for testing or testing scenario.
- h. Choosing the right tools for AVA\_VAN.2 Testing
- i. Collecting data and findings
- j. Recording all findings into one Test Plan

Upon completion of each training module, mentees are required to fill in Section A of Common Criteria Training Evaluation Form to assess their own understanding. Mentors will also fill in Section B of the form to assess their mentee's evaluation competency. Scores are given for each Module together with comments and a total score of 70% and above can be used to show that the mentee is competent. Mentors should state whether the training meets its objectives, whether the mentee is competent, and whether the mentee is recommended to attend further trainings to increase their competency.

In our effort of increasing the competency of our evaluators in doing CC evaluations, we engage with known CC practitioners like Mr. Wouter Slegers of Holland to provide intermediate and advanced CC training. The training not only involved theory, but also hands-on exercises and discussions. These kind of trainings enable us to go deep in discussions and also get proven methods and approach from experienced and knowledgeable people.

In our process of obtaining the ISO 17025 accreditation, which we've successfully obtained end of last year, I was involved in the preparation of our Training Plan and CC Training Module which documents most of the strategies mentioned in this paper.

### **Conclusion**

The strategies discussed in this paper are what CyberSecurity Malaysia MySEF implements in order to ensure our evaluators are competent. We find that they are somewhat effective, and we hope to be able to get feedbacks and recommendations. And, we are sometimes faced with some constraints such as unavailability of budget when we're trying to conduct trainings or when we want to send our evaluators for training. And, there is no specific place for us to get assistance and advice in our effort of increasing our evaluators' level of competency.

### **Recommendation**

We would like to recommend that an institute for CC training is established in order to provide CC training, especially for young schemes like MyCC. We would also recommend a mechanism is introduced whereby senior evaluation facilities can provide assistance to newly established evaluation facilities. These initiatives may help speed up the learning curve and provide solution for the constraints I mentioned which I think might be faced by some other new evaluation facilities too, hence, contributing towards the betterment of CC globally and indirectly increase the security postures globally. We also hope to encourage discussions and recommendations on this topic, for the benefit of all.