Leveraging MyCC Certification to Boost Malaysia's ICT Exports

Companies and governments around the world depend on information and communications technology (ICT) products and services. They rely on ICT for national and economic security, public safety and law enforcement, as well as the confidentiality of their data and the data of the individuals they serve. These users are also increasingly concerned about cyber security risks. In today's digital world, new cyber security risks emerge every hour of every day. Organizations suffering from hacker attacks are susceptible to losing control of confidential data and millions of ringgit in reputational damage and business losses.

The Common Criteria (CC) is an international standard defining a framework for IT security evaluation and certification. It provides value to that customer by having independent third party evaluate and validate these security requirements against recognized industry standard criteria. More so, if that third party is credible and accredited by government certification scheme.

Vulnerabilities in IoT Devices

Technological advancements and proliferation of smart devices are requiring higher security assurance levels due to high cybersecurity risks. According to a recent World Economic Forum (WEF) report, consumer Internet of Things (IoT) market size from wearables to electronics and home appliances is forecasted to reach about US$154 billion by 2028. However, these new ICT products coming onto the market continue to introduce vulnerabilities. The ICT sector is also one of the fastest-growing sectors in Malaysia, which contributed to 19.1 percent of the country's GDP in 2019 and is expected to reach 22.6 percent by 2025.

To ensure a resilient infrastructure for enterprises and safer consumer ICT products, cybersecurity must be an important consideration when companies design their systems and networks. Establishing cybersecurity measures will benefit companies by protecting them from the reputational and financial risks posed by cyber threats; while more cyber robust consumer ICT products will ensure a pleasant user experience free from hackers.

ICT product companies must therefore adopt a Security-by-Design approach which is more cost-effective than implementing cybersecurity measures only after systems have been designed and built. As such, product assurance, whereby products are evaluated and certified based on international standards such as **Common Criteria (CC)**, is a critical step in reducing cyber-attack surface and make the ICT products more marketable.

Defining Security Requirements

As mentioned, Common Criteria (CC) is an international set of standardized guidelines and specifications developed to evaluate information security products. It is a framework in which users specify their security functional requirements (SFRs) and security assurance requirements (SARs) or make reference to **Protection Profiles (PPs)**. Technology vendors can then implement and/or make claims about the security attributes of their products and engage certification bodies to evaluate their products to determine if they meet these claims.

CC provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous, standard and repeatable manner

at a level that corresponds with its target use environment. Once this process is completed successfully, a vendor achieves Common Criteria certification.

Also known as **ISO/IEC 15408,** CC is the internationally recognised standard for information technology security evaluation, while Common Evaluation Methodology (CEM) or **ISO/IEC 18045** constitutes common methodology for information technology security evaluation. Both ISO are the technical basis for the international agreement named as Common Criteria Recognition Arrangement (CCRA).

As of 2019, thirty one countries signed the CCRA, thus making it an unparalleled measure of security for the international commerce of ICT products. Malaysia, through CyberSecurity Malaysia, has been accepted as CCRA Consuming Participant in 2007 and recognized as CCRA Authorizing Participant by 2011. Through the certification program, participants gain access to a global community of technical experts, who together identify and address the threats.

MyCC in Malaysia

In Malaysia, Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme is set up to evaluate and certify the security functionality of ICT products against defined criteria or standards. MyCC Scheme evaluates and certifies the security functionality within ICT products against **ISO/IEC 15408** while the methodology used is **ISO/IEC 18045**. The Certification Body for the MyCC Scheme in Malaysia is **Malaysian Common Criteria Certification Body (MyCB)**, a department within CyberSecurity Malaysia.

Components of Common Criteria

Common Criteria has two key components: Protection Profiles (PP) and Evaluation Assurance Levels (EAL).

PP defines a standard set of security requirements for a specific type of product (examples include firewalls and digital signatures) relevant to that user for a specific purpose. Product vendors can choose to implement products that comply with one or several PPs and have their products evaluated against them.

EAL defines how thoroughly a security product is tested. There are seven Evaluation Assurance Levels (EALs). The higher the level, the more confidence that the security functional requirements will be met. Each EAL corresponds with a package of Security Assurance Requirements (SAR), which covers the full development of a product across a certain level of rigorousness. However, the levels only indicate that more testing was done rather than that the product is more secure.

CC Certification Process

CC addresses protection of information from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called **confidentiality, integrity,** and **availability**, respectively.

CC is presented as a set of distinct but related parts:

Part 1 - Introduction and general model

Part 2 - Security functional components establishes a set of functional components that serve as standard templates upon which to base functional requirements for TOEs.

Part 3 - Security assurance components establishes a set of assurance components that serve as standard templates upon which to base assurance requirements for TOEs.

The first step in submitting an ICT product for CC certification is completing a Security Target description. One needs to include an overview of the product and its security features, an evaluation of potential security threats, and a self-assessment detailing how the product conforms to the relevant **Protection Profile (PP)**, or the **Evaluation Assurance Level (EAL)** chosen to test against.

The second step is to generate assurance documentation that are required for the testing lab. Next, the product and its associated documentation are submitted to an accredited testing laboratory, which tests the product to verify its security features and evaluate how well it meets the specifications outlined in the PP. The results of a successful evaluation form the basis for an official certification of the product.

In Malaysia, evaluation facilities for the MyCC Scheme is known as **Malaysian Security Evaluation Facility (MySEF)**. There are currently five[1] Security Evaluation Facility (SEF) licensed under MyCC Scheme.

The goal of CC certification is to assure customers that the products they are buying have been evaluated and that the vendor's claims have been verified by an independent party.

The Common Criteria certification achieves the following critical objectives:

- **Better Access to Government Tenders**
  Most governments across the globe require Common Criteria certification in their ICT product procurement. As such, Malaysian ICT products which are CC certified will qualify for tender.

- **Enhance Market Competitiveness**
  For better market share access, Common Criteria certification is critical to compete with other well-established IT products which have been evaluated.

- **Products Certification Signals Quality**
  Certification brings a level of quality assurance for enterprise IT buyers. Stringent evaluation process may uncover previously unknown vulnerabilities that can be addressed before sending a product to market, preventing costly post-release patches.

Challenges of CC Certification

ICT product developers need to have a thorough understanding of the requirements in order to prepare the CC documentation and successfully complete the evaluation. Furthermore, a

[1] https://www.cybersecurity.my/mycc/license.html

high level of commitment is required during the evaluation so that the project timeline can be met. Budget could present another challenge for smaller organisations as CC typically involves higher cost for the evaluation facility service and certification.

CC certification enables ICT product buyers to reduce risk by procuring and using products that have sufficient security and integrity for their environments. By factoring security into procurement decisions, buyers in turn incentivize ICT vendors to develop and provide more secure ICT products.

-END-

About Us

Information Security Certification Body (ISCB) is a department established under CyberSecurity Malaysia since 2008. Based on Malaysian Government Cabinet decision, Malaysian Common Criteria Certification Body (MyCB) is established as the sole Certification Body for the Malaysian Common Criteria Evaluation & Certification (MyCC) Scheme.

After 2010, MyCB had evolve it certification services to CyberSecurity Malaysia Information Security Management System Audit and Certification (CSM27001) Scheme and Malaysia Trustmark for Private Sector (MTPS) Scheme. Therefore, MyCB name is changed to ISCB Department as the department role also grown to other areas of certification which is categories under management system, product and personnel certification.

For more information contact us ***certification[at]cybersecurity.my*** *or visit* ***https://iscb.cybersecurity.my.***