7 Steps to Common Criteria Certification

by Lachlan Turner
Partner & Principal Consultant, Lightship Security

Lightship Security

FOREWORD

This ebook presents the broad steps towards achieving Common Criteria certification. They're not strictly linear but are more of a general guide as to the key decision points and activities that occur throughout the process.

My name is Lachlan Turner and I'm the Principal Consultant at Lightship Security. At Lightship, we are working hard to continually optimize the certification experience for our clients. Leveraging our own intelligent automation tools, extensive pre-validation process and our intimate knowledge of the standards, we focus on reducing our client's certification costs, schedules and time to market.

www.lightshipsec.com

TABLE OF CONTENTS

WHAT IS COMMON CRITERIA?

The Common Criteria (CC) is an international standard for evaluating the security functions of IT products. It defines a framework for the oversight of evaluations, syntax for specifying the security requirements to be met and a methodology for evaluating those requirements. CC evaluations are intended to provide consumers with a defined level of independent assurance in the secure operation of a certified product.

The “Common” in Common Criteria is there because the CC is a mash-up of multiple countries’ IT security evaluation criteria. The genesis and sustaining reason for the CC’s existence is policy — government agency procurement policies around the world that require products to be CC certified. Vendors are incentivized through sales to achieve compliance. Before the CC, each country had its own evaluation criteria whereas now vendors can be evaluated once and recognized world-wide.

The CC defines seven Evaluation Assurance Levels (EAL) which provide a sliding scale of assurance from EAL1 (lowest) to EAL7 (highest). However, the Common Criteria Recognition Arrangement (CCRA) has capped mutual recognition at EAL2 except in the case of internationally recognized Collaborative Protection Profiles (cPP) in which case assurance components up to EAL4 may be incorporated in the cPP. The CC standard documents can be obtained from **www.commoncriteriaportal.org**.

Here are the answers to the top questions about Common Criteria:

1. How much does Common Criteria certification cost?

A CC evaluation, including lab and consulting fees, can vary greatly depending on the claims, complexity of testing and number of models tested. It is safe to assume that the cost will be north of USD $100k. There are multiple factors to consider that impact this amount.

2. How long does Common Criteria certification take?

The general rule of thumb is about one year including preparation time using the legacy approach. Uniquely, Lightship Security has demonstrated through our test automation solutions and accredited laboratory that evaluations can be completed in 2-3 months from end to end.

3. What gets evaluated under Common Criteria?

Traditionally, Common Criteria evaluation consisted of large amounts of documentation review with a small amount of testing. The latest Protection Profiles however place more emphasis on functional testing.

The mud-map of evaluation looks like this:

- **Security Target evaluation.** Evaluation of the Security Target (ST) - a claims document that specifies the functions under evaluation and the assurance requirements being met.
- **Design evaluation.** Evaluation of design documents - at the most basic level this will simply be an interface specification. Depending on the assurance requirements this can include multiple layers of very detailed design specs and source code review (this is becoming less common).

- **Guidance evaluation.** Evaluation of all the guidance documents that are shipped with the product and a CC specific addendum or 'Secure Installation Guide' for achieving the evaluated configuration.
- **Life-cycle evaluation.** Evaluation of configuration management practices, delivery procedures and security bug tracking (flaw remediation). Can also include development practices and site security audits.
- **Functional testing.** The evaluators repeat a sample of the developer's functional tests and come up with some independent tests to confirm the operation of the security functions as specified.
- **Penetration testing.** The evaluators will try to identify and exploit vulnerabilities.

Whether a particular evaluation activity gets performed is dependent on the assurance requirements that are specified in the Security Target. EAL levels are simply pre-canned packages of assurance requirements.

Evaluation activities for the latest Protection Profiles focus on the Security Target, Guidance and Functional Testing.

4. What is a Security Target?

A Security Target is the document that defines the Target of Evaluation (TOE), that is, the product configuration and version, and scope of security functionality being evaluated. The CC allows the TOE to be all or part of a product or system. The Security Target is put together using CC constructs. As with a Protection Profile (see below), the Security Target defines both functional requirements as well as assurance requirements. A Security Target may conform to a Protection Profile but is not required

to. A Security Target (written by vendor) goes beyond a Protection Profile (written by consumer) by including a description of how the product achieves the defined requirements. There are plenty of Security Target examples at **http://www.commoncriteriaportal.org/products.html**

5. What is a Protection Profile?

A Protection Profile is a requirements statement put together using CC constructs. They are generally published by governments for a specific technology type, like Firewalls for example, as part of procurement policy. A Protection Profile specifies both functional requirements as well as assurance requirements. EALs specify the assurance part - so a Protection Profile may reference an EAL or list of assurance requirements but will also specify a set of functional requirements to be met. By far the most commonly used Protection Profiles are those published by the United States **National Information Assurance Partnership (NIAP)**. In addition to these, work on internationally agreed Protection Profiles is published at the **Common Criteria Portal**.

Now that you have a good understanding of Common Criteria, here are the steps to achieving CC Certification.

STEP 1: UNDERSTAND WHAT YOU SHOULD COMPLY WITH

This step is important because it will to a large extent determine the cost of certification and whether it is a worthwhile exercise that leads to a return on investment. Most vendors will have a specific sale or market segment that drives the need for certification. In such cases, the requirement has traditionally been to get certified at EALx – where x was driven by the consumer, who was driven by security/procurement policy. This may still be the case in some countries and yet in others EAL evaluations are no longer performed in favor of Protection Profiles.

Answers to the following questions will aid in defining your requirements:

- **What assurance package is required?** Determine if there is a specific Protection Profile, EAL or other 'named package' of requirements that must be met. **Note:** If the primary market is U.S. federal, then you will likely need to be on the NIAP Product Compliance List (PCL) which requires conformance with a **US Government Protection Profile**.
- **What functional components are required?** If a Protection Profile is required then this question has already been answered, otherwise, determine if there needs to be any specific security functions included in the scope of evaluation.
- **What is the actual policy driver?** It may be useful to know what the specific policies are that drive your customers to request Common Criteria.

If there is more than one customer or market segment that requires Common Criteria, it will be necessary to understand the requirements for each to enable strategic planning of the resulting evaluation effort(s). As with most of the steps, a good lab or consultant should be able to help with this process – most should be willing to get you moving in the right direction as part of pre-sales discussions. You might even try engaging with the **Common Criteria schemes** in your target countries for assistance with this step.

STEP 2: DECIDE WHICH SCHEME

At the time of writing, schemes that issue certificates include Australia, Canada, France, Germany, India, Italy, Japan, Malaysia, Netherlands, New Zealand, Norway, South Korea, Spain, Sweden, Turkey, United Kingdom and the United States. The current list is published at the **CC Portal CCRA Members page**.

Having a choice of schemes and countries for evaluation is becoming a key decision point for a lot of vendors for one fact – simply getting into evaluation is increasingly difficult. Each scheme enforces different rules for acceptance of a product into evaluation in-line with the national interest.

Here are the following factors to consider when choosing a scheme:

- **Product market.** Most vendors will be selling into federal government markets – the defense market for example. Such vendors will need to ensure the selected scheme is able to support the market's procurement policy requirements – such as accommodating a **US Government Protection Profile**. For other vendors who are not selling to such markets – the commercial telecommunications market for example – scheme selection can be thrown open to wherever is cheapest or has the most flexible entry requirements.
- **Competitors.** For some vendors, being listed on the same scheme web site as a direct competitor is very important, and therefore drives scheme selection. When a certificate is issued, a listing will

be posted on the country's scheme web site and then subsequently posted to the Common Criteria portal site at **http://www.commoncriteriaportal.org/products/**

Note: when conforming to a US / NIAP Protection Profile, the evaluation may still be performed outside of the US. Once the evaluation completes, there is a scheme-to-scheme process to have the product listed on the US / NIAP **Product Compliant List**. NIAP will perform a review and may require changes prior to posting to the PCL.

- **Scheme reputation.** For those who have worked with a few different schemes, there definitely different 'styles' of certification / validation (the function of the scheme). As with any organization scheme certification bodies can be efficient or not, heavy handed or reasonable in policy enforcement, slow, fast, simple, complex etc. Other vendors who have been through the process may also provide good insight here – the **Common Criteria User Forum** is a great place to ask such questions.

Lightship Security performs Common Criteria evaluations within the Canadian Common Criteria scheme which accepts evaluations up to EAL2+ and Protection Profile based evaluations (which are listed on the NIAP PCL once complete). We provide access to other schemes through our lab partnerships.

STEP 3: CONFIRM THE SCOPE

Common Criteria evaluation will typically consider a subset of the security functions, configurations and models of a product – primarily because it is necessary to bound the evaluation effort to focus on aspects that are most relevant to the certified product consumer. This section provides guidance on deciding on the scope.

When conforming to a Protection Profile it will not be necessary to define the scope of functions to evaluate (as these are specified by the Protection Profile), however, it will be necessary to consider which flavor of your product to certify (i.e. models / supported OS etc.) and the specific configuration.

When not conforming to a Protection Profile, it will be necessary to specify those security functions that will be within the scope of evaluation – these are then expressed as security functional requirements in the Security Target.

The following factors should be considered when deciding on scope:

- **Subset.** It is generally not necessary or beneficial to include all security functions within scope of an evaluation – it is better to focus on a well-defined subset relevant to the certified product market.

- **Scheme policy.** Schemes will often have requirements around the scope of an evaluation, such as requiring the ‘core security functions’ as advertised to be included in scope. In addition, schemes will generally have requirements around cryptography – how this can be specified and what protocols and algorithms are allowed.
- **Common use cases.** Consider the most commonly used models, configurations and functions for evaluation.
- **Competitors.** If a competitor with a similar product has already been through evaluation, it might be worth downloading their Security Target from **www.commoncriteriaportal.org** to see what claims they made.

Your consultant, lab or scheme can provide valuable guidance for this step.

STEP 4: IDENTIFY AND MITIGATE COMPLIANCE GAPS

In preparing to undertake evaluation, especially when conforming to a Protection Profile, it is critical to address gaps that may exist in the following areas:

- **Functionality.** When conforming to a Protection Profile it is important to confirm that your product implements the specified security functional requirements – these will be found in the Security Functional Requirements section of the Protection Profile and are mandatory to implement.
- **Life-cycle processes.** These are documented procedures for configuration management, product delivery, development security, development tools documentation, development methodology and flaw remediation. At the lower end of assurance (up to EAL2 or equivalent), most vendors will already have the required configuration management and secure delivery processes in place. The other requirements only kick in above EAL2, or as explicitly stated in the assurance requirements of a Protection Profile. At these higher levels of assurance, it is common for the processes to be in place but for documented procedures to be lacking.

Experience has shown that 100% of vendors will initially fail NIAP / Collaborative Protection Profile testing due to the onerous and very prescriptive nature of the testing. These missed gaps often result in expensive last-minute code fixes, delayed certification and delayed time to market. At Lightship, we have developed a widely used Functional Gap

Analysis (FGA) approach – that comprehensively and transparently exercises the product against the requirements using Greenlight, our conformance automation platform. The output of the FGA can be used to provide certainty to our clients about the conformance of their product. This approach dramatically reduces the overall risks in the certification process. Areas where vendors are most likely to fail testing include:

- Audit requirements
- X.509 certificate validation
- TLS implementations
- SSH implementations

STEP 5: ENGAGE A LAB

Most Common Criteria schemes will license commercial facilities / labs within that country to perform evaluations. Vendors engage directly with the lab which then interacts with the scheme. Vendors can and should begin discussions with potential labs right from Step 1. Good labs will provide valuable information during pre-sales discussions to assist vendors through Steps 1 – 4 and will likely offer consulting services to assist with these phases.

Lightship Security is a lab within the Canadian Common Criteria scheme.

STEP 6: SUPPORT THE EVALUATION

Probably the most critical step for a fast evaluation is that your consultant and lab will need good access to product and QA engineers who can describe how the product works, provide existing design documentation (if any) and explain the in-house testing methodology. It's best if the certification project lead has sufficient influence to tap these resources as required. I've been involved in many evaluations that bog down simply waiting for input. Access to engineers will peak during the documentation development and testing phases.

The typical flow of an evaluation will be:

1. **Acceptance**
2. **Documentation Review**
3. **Testing**
4. **Certification / Validation**

Once the lab completes 1 through 3, they submit a final report to the scheme / Certification Body. The amount of turnaround time at this point (4) is dependent on the scheme work load and approach – Canada and U.S. typically take around four to six weeks before you'll get the final certificate.

STEP 7: MAINTAIN CERTIFICATION

Once you have gained certification, it makes sense to leverage the value of this initial investment to maintain certification over time. Within the U.S. certificates are removed from the PCL after 2 years. Internationally, certificates are deemed invalid after 5 years. This does not mean that you should wait until your certificate becomes invalid before embarking on another evaluation. It is preferable to plan a regular cadence of re-certification that allows each certification effort to build on the one before. This approach allows for maximum reuse of previous evaluations and ensures that your clients always have a path to procure certified versions of the latest and greatest technology.

At Lightship, our goal is certification at the speed of development. We enable this through Greenlight, our conformance automation platform which allows vendors to embed Common Criteria testing into their own QA process. By using Greenlight throughout the product lifecycle in this way, vendors can be assured that code changes have not broken their certified functionality – this in turn allows for efficient re-certification and faster time to market.

Be sure to engage with your consultant and/or lab to establish a certification roadmap that aligns with your product roadmap for maximum ongoing value in your certification efforts.

ABOUT THE AUTHOR

Lachlan leads the professional services practice for Lightship Security. He has worked in government certification roles, led evaluation teams for multiple test labs and has assisted many vendors through the Common Criteria evaluation process as an independent consultant. Lachlan holds CISSP and CRISC designations and is a member of the Common Criteria Users Forum (CCUF) Management Board.

ABOUT LIGHTSHIP SECURITY

Lightship Security is an IT security laboratory specializing in conformance automation software solutions and security certification services. We support our client's entire validation and certification needs for Common Criteria, FIPS 140-2 and other internationally required standards.

Lightship's mission is to enable certification at the speed of development. Our approach is to move the certification process closer to the development team using smart automation and our pre-validation processes to make the certification process easier. Our clients benefit by getting their latest certified technology to market faster.

www.lightshipsec.com


Lightship Security