7 Steps to Common Criteria Certification

Lightship Security

Applus+

FOREWORD

This book outlines the essential stages on the path to Common Criteria certification. The process isn’t strictly linear. Instead, think of these steps as a strategic guide to the critical decisions and activities that shape a successful evaluation from start to finish.

Certification is changing fast, and vendors deserve a process that keeps up with the pace of innovation. At Lightship Security, we’ve made it our mission to help organizations turn certification from a bottleneck into a competitive advantage. Through intelligent automation, deep standards expertise, and a relentless focus on efficiency, we’re raising the bar for what modern certification can—and should—look like.

Lightship Security
Applus+

www.lightshipsec.com

TABLE OF CONTENTS

WHAT IS THE COMMON CRITERIA?

The Common Criteria (CC) is an international standard (ISO/IEC 15408) 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 reflects the unification of what were once separate national IT security standards. Instead of navigating a patchwork of country-specific requirements, vendors now follow a consolidated, streamlined framework. Because many government and commercial procurement programs mandate CC certification, achieving compliance offers both market access and strong competitive advantage.

The introduction of the European Union’s CC scheme ‘EUCC’ is the latest industry development.   EUCC uses the same CC standard but includes some additional elements such as post-certification vulnerability management that is specific to the EU market. Step 2 below provides a deeper analysis of the impact of EUCC.

The CC defines seven Evaluation Assurance Levels (EALs) which provide a sliding scale of assurance from EAL1 (lowest) to EAL7 (highest). EAL2 and EAL4 are common, with custom packages of requirements in the form of Protection Profiles becoming more prevalent.

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

1. How much does Common Criteria certification cost?
Common Criteria evaluation is a substantial investment, typically ranging into the hundreds of thousands of dollars. Exact costs vary based on several factors, including the chosen EAL / Protection Profile, product complexity, evaluation scope, and the level of vendor preparedness.

2. How long does Common Criteria certification take?
A typical Common Criteria certification takes around a year from initial preparation to final approval, though timelines can vary widely. Factors such as product complexity, evaluation scope, and the readiness of documentation and testing all play a role. With the right preparation and support, many vendors are able to shorten this timeline significantly.

3. What is NIAP and the PCL?

NIAP (the National Information Assurance Partnership) is the U.S. government authority responsible for managing Common Criteria evaluations and approving Protection Profiles in the U.S. The Product Compliant List (PCL) is NIAP's official list of products that have successfully completed evaluation against an approved NIAP Protection Profile and are recognized for U.S. government procurement.

4. What is a Protection Profile?
A Protection Profile is a security requirements statement put together using CC constructs. They are generally published by governments or user communities for a specific technology type, like Network Devices for example. A Protection Profile specifies both functional requirements (e.g.

product must do XYZ) as well as assurance requirements (e.g. evaluator must test XYZ). EALs only specify the set of assurance requirements.

5. What is a Collaborative Protection Profile?

A Collaborative Protection Profile (cPP) is a PP that has been developed by an International Technical Community (iTC) according to a process that allows nations to signal endorsement of the cPP.

6. What is a Security Target?

A Security Target is the document that defines the Target of Evaluation (TOE) and related conformance claims. The TOE is the thing being evaluated, identified by the product name and version and encompassing the scope of security functions being evaluated. The CC allows the TOE to be all or part of a product or system. 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.

7. What gets evaluated under Common Criteria?

A high-level view of the evaluation process looks like this:

- **Security Target evaluation.** Review of the Security Target (ST) - a claims document that specifies the functions under evaluation and the assurance requirements being met.
- **Design evaluation.** Assessment of design documentation—ranging from basic interface specifications (e.g. EAL2) to, in some cases, deeper design layers or source code review (e.g. EAL4).

- **Guidance evaluation.** Review of all product guidance delivered to customers, including any CC-specific addendum or Secure Installation Guide required to achieve the evaluated configuration.
- **Life-cycle evaluation.** Examination of configuration management, delivery procedures, flaw remediation, and—depending on the assurance level—development practices and site security.
- **Functional testing.** Re-execution of a subset of the developer's tests along with independent evaluator tests to confirm correct operation of the claimed security functions.
- **Vulnerability assessment.** Identification, analysis and testing of potential vulnerabilities.

The specific set of activities performed depends on the assurance requirements defined in the Security Target. EALs simply package these assurance requirements into predefined sets. For NIAP Protection Profiles and Collaborative Protection Profiles, the evaluation focus is primarily on the Security Target, guidance, functional testing and vulnerabilities.

8. How does FIPS140 relate to Common Criteria?

FIPS140-3 is a U.S. and Canadian government standard that defines security requirements for cryptographic modules. Cryptographic Module Validation (CMVP) is not required for CC.

However, there are two closely related types of validations that are often required for CC in North America:

- **Cryptographic Algorithm Validation (CAVP).** Validates that *cryptographic algorithms themselves* (AES, SHA, RSA, etc.) are implemented correctly.
- **Entropy Source Validation (ESV).** Validates the design and behavior of entropy sources—the components responsible for generating randomness used in cryptographic operations.

Schemes outside of North America may or may not recognize FIPS140.

STEP 1: CLARIFY YOUR CERTIFICATION DRIVER

This step is important because it will largely 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 opportunity or market segment that drives the need for certification.

Answers to the following questions will aid in providing clarity:

- **What certified product list(s) do we need to be on?** This is the critical question to answer. Typically, one or more of:
  - NIAP Product Compliant List
  - Commercial Solutions for Classified (CSfC) Components List
  - International Common Criteria Portal
  - ENISA EU Cybersecurity Certificates (EUCC)
  - Other national specific product list
- **What conformance claims are required?** Determine if there is a specific Protection Profile or EAL that must be met.
- **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.

STEP 2: DECIDE YOUR SCHEME STRATEGY

Your scheme strategy will identify where to perform your evaluation project. A Common Criteria ‘Scheme’ refers to the CC ecosystem in a given nation or group of nations (e.g. EU). Each Scheme has its own policies and rules for how they implement CC (e.g. how labs are accredited, how evaluations are monitored etc.). Schemes must implement agreed baseline requirements to be able to participate in Mutual Recognition Arrangements or Agreements (e.g. Common Criteria Recognition Arrangement (CCRA)). Examples Schemes include: NIAP in the U.S., the Canadian Common Criteria Scheme, the Australian Information Security Evaluation Program (AISEP) and the EUCC Certification Scheme.

Before the introduction of EUCC, the terms Scheme and Certification Body (CB) were essentially synonymous. The EUCC Scheme introduces:

- **National Cybersecurity Certification Authority (NCCA).** The government body in each EU Member State responsible for supervising cybersecurity certification.
- **Conformity Assessment Body (CAB).** Commercial or government entities acting as:
    - Evaluation CABs (aka labs)
    - Certification CABs (aka CBs)

In addition, EUCC has introduced post certification surveillance of certificates (a sample of certificates will be audited for ongoing conformance) and post certification vulnerability management and reporting. This means that certification under EUCC is not a one-and-done prospect, but an ongoing commitment for vendors.

This has created two main types of CC certificates: EUCC certificates and CCRA certificates. Navigating this dynamic is a critical strategic challenge, particularly for vendors who need to address both markets. It is advantageous to work with labs who are accredited in multiple regions and can provide guidance on the best strategy when it comes to Scheme selection.

Here are some factors to consider when developing your Scheme / CB strategy:

- **Certification driver.** What is the primary driver? Based on the answers from Step 1, a short list of Schemes / CBs should become obvious.
- **CCRA, EUCC or both.** In some cases, the best strategy may require two Schemes (e.g. parallel or sequential efforts). This depends on a few factors:
    - The state of EUCC <-> CCRA mutual recognition, which is in flux
    - Recent / previous certifications of the same product
    - Timing / priority considerations
    - Multi-region lab efficiencies
    - Risk reduction -> decouple CCRA (minimal post certification monitoring / risk) and EUCC certificates (heavy post certification monitoring / risk).
    - Version staggering for overlapping certification coverage
- **Scheme / CB rules.** Understand that every CB has its own set of policies and quirks that should be taken into consideration. Below are some examples:

    - **Acceptance rules** – Most CBs have project acceptance rules. For example, NIAP does not accept any EAL projects, whereas Canada does. Evaluation scope is also usually scrutinized to ensure it includes core security functions.
    - **Project timelines** – Prescribed deadlines to achieve certain milestones or risk ‘de-listing’ or project cancellation.
    - **Certification fees** – Some CBs charge fees, others don’t.
    - **Cryptographic requirements** – Approved algorithm and entropy requirements, which may require related certificates (e.g. CAVP, ESV etc.). Some CBs are more flexible than others in this regard.
    - **Certificate validity** – How long does the certificate last? This can vary between Schemes.
- **Scheme friction.** Some CBs can be difficult to deal with or have capacity issues while others can be more efficient and pragmatic – ask around about these factors to weigh up the pros and cons in an informed manner. This aspect tends to change over time so be sure to get input based on recent experiences.

STEP 3: DEFINE THE SCOPE

A Common Criteria evaluation rarely covers every security function, configuration, or deployment model of a product. Instead, evaluations are deliberately scoped to focus on the aspects most relevant to the intended certified product consumer, while keeping the evaluation effort practical, timely, and cost-effective.

This section provides guidance on how to define an appropriate evaluation scope.

When conforming to a Protection Profile (PP), the security functionality in scope is largely predefined by the PP itself. However, vendors must still decide which product variants will be included in the evaluation—such as specific models, supported operating systems, and deployment configurations. These decisions apply equally to both PP-based and EAL evaluations.

Defining the Physical Scope

The following factors should be considered when defining the physical scope of the evaluation (for example, models, operating systems, and form factors):

- **Time and Cost.** Expanding the number of configurations included in scope typically increases evaluation duration and cost. Certification schemes apply equivalency rules conservatively, which often limits the ability to test one configuration and claim coverage for others. Common drivers of increased effort include:

    - Hardware models based on different CPU microarchitectures
    - Hardware variants with different cryptographic accelerators or chips (e.g. MACSEC implementations)
    - Virtual appliances deployed on different hypervisors
    - Applications running on different operating systems
- **Certification Driver.** Re-anchoring on the original certification objective often reveals that a streamlined physical scope is sufficient to meet market, customer, or regulatory requirements.
- **Phased Expansion Strategy.** Many vendors benefit from certifying an initial, streamlined configuration and expanding coverage over time through assurance continuity or re-evaluation as customer demand evolves.

Defining the Security Functional Claims (e.g. EAL)

When not conforming to a Protection Profile, it will be necessary to specify the 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 functional scope:

- **Focused Subset.** Including every available security feature is rarely necessary or beneficial. Evaluations are most effective when scoped to a clearly defined subset of functions aligned with the intended certified market.

- **Scheme policy.** Schemes often impose requirements on evaluation scope, such as mandating inclusion of *core security functions* as advertised. Schemes also apply specific rules around cryptography, including permitted algorithms, protocols, and how cryptographic claims may be expressed.
- **Market benchmarking.** Reviewing publicly available Security Targets from comparable products can provide valuable insight into typical scoping decisions. These can be accessed via public certification lists.

STEP 4: FIND AND CLOSE COMPLIANCE GAPS

When preparing for an evaluation—particularly one that claims conformance to a Protection Profile—it is essential to identify and address potential gaps early in the following areas:

- **Functionality.** For Protection Profile conformance, vendors must confirm that their product implements all mandatory Security Functional Requirements (SFRs) defined in the Protection Profile. These requirements are non-negotiable and are assessed strictly during evaluation.
- **Life-cycle processes.** Evaluations also assess documented life-cycle processes, including configuration management, secure product delivery, development security, development tools documentation, development methodology, and flaw remediation. At lower assurance levels (up to EAL2 or equivalent), most vendors already have adequate configuration management and delivery processes in place. Additional life-cycle requirements typically apply only above EAL2, or where explicitly mandated by a Protection Profile. At higher assurance levels, vendors often have the necessary practices in place operationally, but lack the formal documentation required to satisfy evaluation criteria.

In practice, experience shows that nearly all vendors initially fail NIAP or Collaborative Protection Profile testing due to the highly prescriptive nature of the test requirements. Unidentified gaps frequently lead to latestage code changes, increased costs, certification delays, and slower time to market.

To mitigate this risk, Lightship has developed a widely adopted Functional Gap Assessment (FGA) approach. Using our Greenlight Conformance Automation Platform, we execute the most critical Protection Profile tests before the formal evaluation begins. This early validation significantly reduces certification risk and prevents costly surprises later in the process.

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 and U.S. Common Criteria schemes, and is a wholly owned subsidiary of Applus+, a global testing, inspection, and certification organization with decades of experience supporting regulated industries worldwide. Through Applus+'s accredited conformity-assessment operations — including accreditation to perform EUCC evaluations — Lightship is able to pair its deep, hands-on Common Criteria expertise with the scale, governance, and regulatory credibility of a multinational TIC organization actively engaged with European cybersecurity certification frameworks.

STEP 6: SUPPORT THE EVALUATION

This is the most critical factor in a successful evaluation. The lab must have timely access to product and QA engineers who can clearly explain how the product works, share available design documentation, and describe internal testing processes. It’s important that the certification project lead has enough authority to engage these resources as needed. In many evaluations, progress slows not because of technical complexity, but simply due to delays in receiving required input. Engineer involvement is typically heaviest during the documentation development and testing phases.

A Common Criteria evaluation generally follows this sequence:

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

Once the lab completes the first three phases, a final report is submitted to the scheme or Certification Body. Turnaround time for the certification or validation phase varies by scheme and workload.

STEP 7: MAINTAIN CERTIFICATION

Once certification is achieved, it's important to maximize the return on that initial investment by planning for certification continuity over time. In the U.S., certificates are typically removed from the Product Compliant List after two years, while internationally, certificates are generally considered invalid after five years. This does not mean organizations should wait until a certificate expires before starting a new evaluation. A far more effective approach is to establish a regular re-certification cadence, allowing each evaluation to build on the last.

This strategy enables maximum reuse of prior evaluation artifacts and ensures that customers can continuously procure certified versions of current, market-relevant technology.

At Lightship, our objective is certification at the speed of development. We support this through Greenlight, our Conformance Automation Platform, which enables vendors to integrate Common Criteria testing directly into their existing QA processes. By using Greenlight throughout the product lifecycle, vendors gain ongoing assurance that code changes have not impacted certified security functionality—resulting in more efficient re-certification cycles and faster time to market.

To realize the greatest long-term value, vendors should work closely with their consultant and/or lab to define a certification roadmap that aligns with their product roadmap, ensuring certification remains an enabler rather than a bottleneck.

ABOUT LIGHTSHIP SECURITY

Lightship Security is a leading cybersecurity assurance and certification lab, helping technology vendors navigate complex global certification frameworks with confidence and speed. Trusted by product teams across networking, infrastructure, and embedded systems, Lightship combines deep technical expertise in Common Criteria, FIPS 140-3, EUCC, and related schemes with a highly pragmatic, engineering-first approach. Our focus is simple: make certification predictable, repeatable, and aligned with modern product development—not a blocker to innovation.

Lightship Security is a wholly owned subsidiary of Applus+, a global testing, inspection, and certification organization operating across highly regulated industries worldwide. Through this relationship, Lightship pairs hands-on cybersecurity expertise with the scale, governance, and international credibility of a multinational TIC leader that is also accredited to perform EUCC evaluations. Together, Lightship and Applus+ enable vendors to achieve and maintain trusted cybersecurity certifications efficiently, globally, and at the pace of real-world development.

Lightship Security