Common Criteria Readiness Assessment

Common Criteria (CC) is the only international security standard for evaluation and certification of IT products. Common Criteria is also an acknowledged ISO standard (ISO/IEC 15408) and is used by public authorities and companies to assess the security and quality of an IT product.

The process to evaluate and certify IT products can be described in three steps:

- A developer develops an IT product. The security claims for this product are specified in a document called the Security Target.
- An accredited lab evaluates the product, according to the claims in the Security Target using the Common Criteria. The accredited lab document the assessment in evaluation reports.
- A certification body verifies that the lab worked correctly and certifies the product based upon the Security Target and the reports provided by the accredited lab. The certification body will issue a certificate and a certification report.

Readiness Assessment provides

- Overview of the Common Criteria
- Evaluation strategy
- Identification of potential deficiencies
- Estimated effort for evaluation

Purpose of the Readiness Assessment

Common Criteria Readiness Assessment is performed to determine if and how the product could be CC evaluated and certified, which parts and security functions should be covered by the evaluation and which additional effort is required for an evaluation. The targeted assurance level can be decided after the readiness assessment.

Procedure

atsec interviews personnel and reviews product and development process documentation to determine the status of the product as well as to estimate any changes needed and effort required. The interviews are performed virtually or at the developer site during a two-day workshop.
This is organized and planned by atsec sending a draft agenda for the workshop and a list of requirements and questions to be answered during the interviews.

During the workshop, atsec together with the developer examine security functionality, physical and logical boundaries for a possible evaluation. atsec also provide an overview of the Common Criteria providing information about the complete evaluation and certification process.

The following documentation is reviewed during the readiness assessment, if available:

- Design documentation such as functional specification and high-level design
- Guidance documentation (user, administrator, installation and start-up guides)
- Development environment documentation including a description of the development tools, configuration management procedures and tools, acceptance procedures, security provisions within the development environment, delivery procedures.
- Life cycle support including descriptions of the Configuration Management Systems (CM system), used during product development, customer delivery and bug tracking. In evaluations at higher assurance levels, also the tools used in the product development are reviewed.
- Test documentation including information about security testing, testing environment, descriptions of any manual or automated test.

Evaluation Strategy

Not all of the requirements are expected to be fulfilled when performing Common Criteria Readiness Assessment. For this reason, it is important to determine all deviations and estimate the effort to

have them corrected. Based on outcome of the Readiness Assessment, an evaluation strategy will be provided.
The evaluation strategy will contain the scope of the target of evaluation (TOE), the security functions and a recommendation of an appropriate Evaluation Assurance Level, even if there cannot be any commitments about the success of a certification.
The evaluation strategy will also contain suggestions regarding selection of the Certification Body.
atsec is accredited to do evaluation under the schemes in Sweden, Germany, Italy, Singapore and the US. To date, atsec has successfully performed more than 175 CC evaluations. The suggested Certification Body will be suggested based on the marketing needs, national or internal approval demands, and also product type.

Deliverables by atsec

There are two deliverables provided by atsec as part of the Readiness Assessment: a report and a presentation.

- The Readiness Assessment report will describe the evidence required for each assurance aspect of the chosen assurance level. It will identify presented information, any deficiencies and estimated efforts to address the gaps. atsec will document the estimated efforts for the developer to go from the current status to a fulfillment of the Common Criteria requirements in the report.
  The report will cover all evaluation aspects, especially all the assurance aspects of the chosen assurance level (e.g., EAL2 and EAL3).
- The presentation will summarize results of the Readiness Assessment.

Other services offered by atsec

Common Criteria is one of many security services we offer. For more information on what other services atsec offers, please visit: www.atsec.se

For more information on how we can help you or other questions about Common Criteria, please contact us at info-se@atsec.com

More information on Common Criteria

If you are interested in knowing more about Common Criteria, please visit:
www.commoncriteriaportal.org

For more information on CSEC, the Swedish Certification Body for IT Security, please visit:
www.fmv.se/csec

atsec information security
atsec information security was founded in 2000 and is an independent, standards based security consultant and security company based in Danderyd, Stockholm. We also operate internationally, in Germany, the US, China and Italy and we have performed many successful projects with different companies and authorities. Our more than 80 employees have extensive international experience and technical expertise within the areas of information security and IT security.

www.atsec.se
info-se@atsec.com
©2021 atsec information security AB