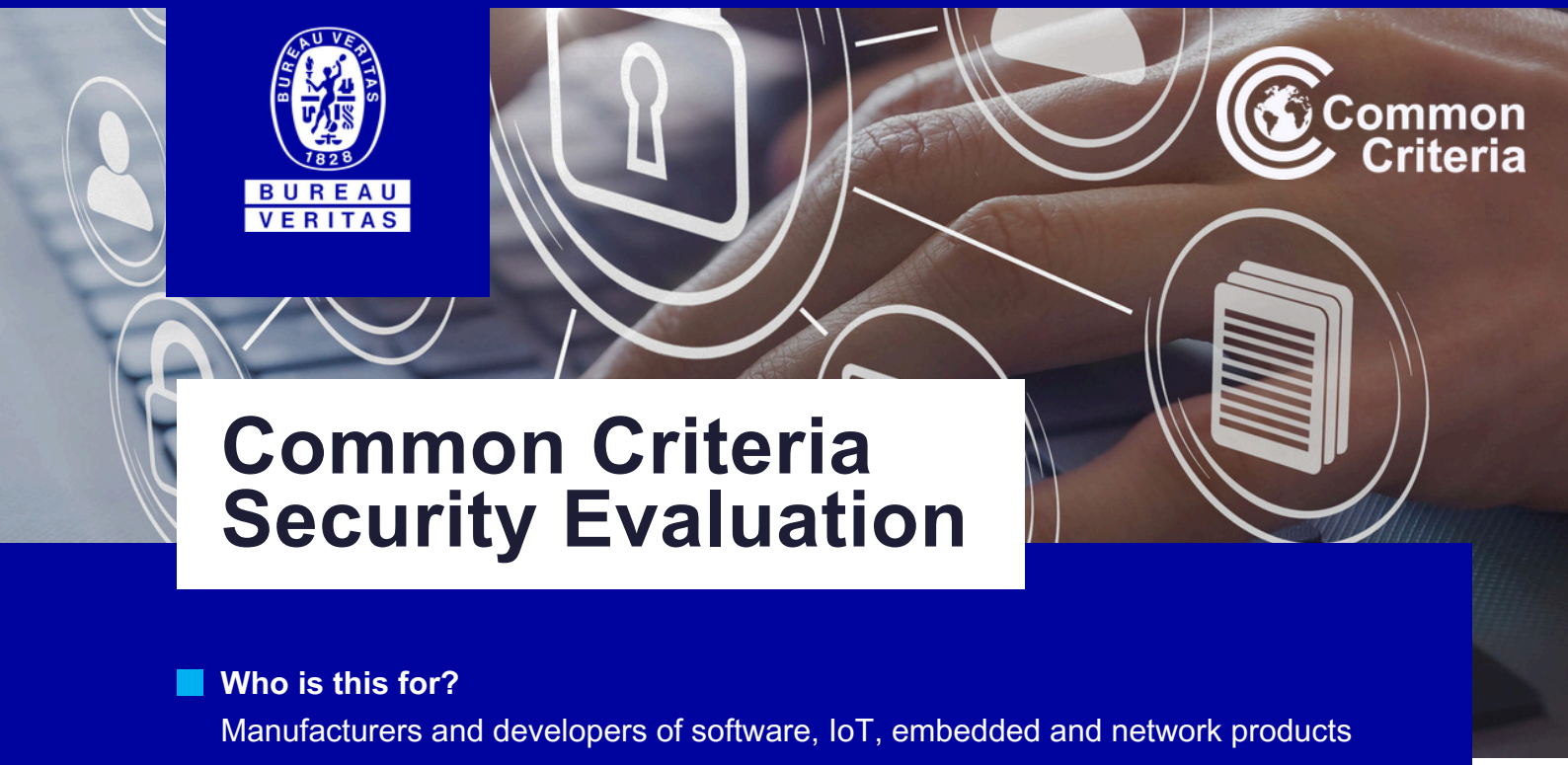
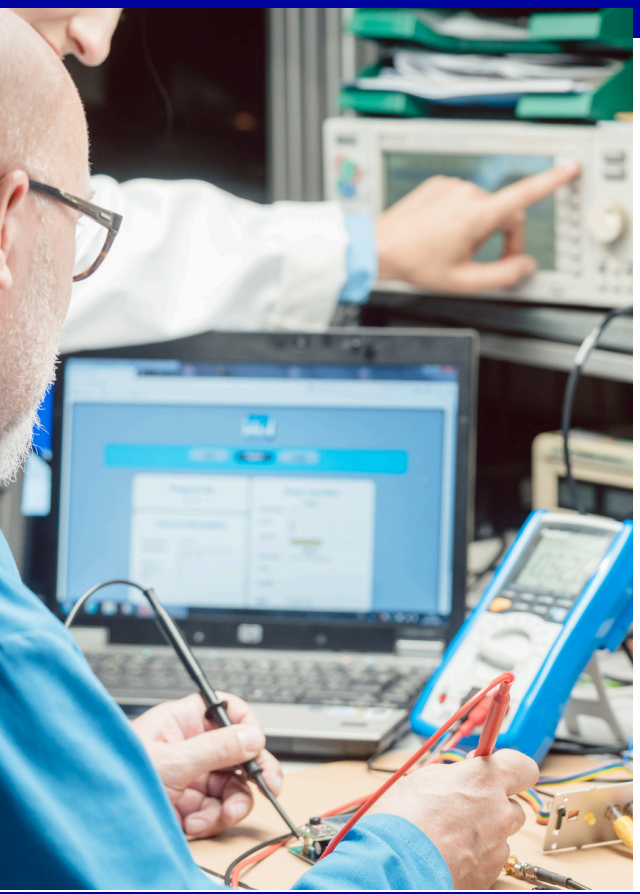


Common Criteria Security Evaluation

Who is this for?
Manufacturers and developers of software, IoT, embedded and network products seeking cybersecurity certification and international market recognition.

What business challenge does it solve?
Demonstrate product security and support market access.

What is the result?
An internationally recognized Common Criteria certificate.



What is Common Criteria?

Common Criteria (CC) is the internationally recognized cybersecurity certification framework for IT, IoT and OT products.

A Common Criteria certificate demonstrates the security assurance of a product through an independent evaluation process. Certified products benefit from international recognition through the Common Criteria Recognition Arrangement (CCRA), supporting access to government, telecom, critical infrastructure and other security-sensitive markets.

Bureau Veritas Cybersecurity performs Common Criteria evaluations under the Dutch Authority RDI. We support organizations throughout the certification journey, from preparation and documentation to evaluation and certification support.

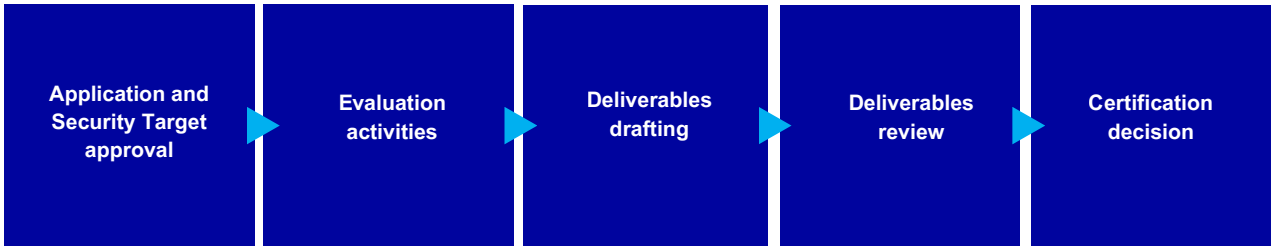
Scope of Evaluation

Common Criteria certification applies to a broad range of software and hardware products that provide security functionality. It is particularly valuable for products sold into government, telecom, critical infrastructure, financial services and other security-sensitive markets where independent security assurance is required. The TOE (Target of Evaluation) in a Common Criteria assessment can be a wide variety of software and hardware products, as summarized in the table below.

Product Category	Product Category
Access Control Devices and Systems	VPN, file encryption, Access control systems, etc.
Boundary Protection Devices and Systems	Data diodes, VPN gateways, Intrusion detection systems, etc.
Data protection	Data encryption tools, Data erasure tools, Data storage tools, etc.
Databases	Database software and applications
Detection devices and systems	Antivirus software, etc.
Smart cards and similar devices	Secure ICs, JavaCards, transportation/access cards, etc.
Key management systems	Secure key management tools
Mobility	Mobile applications
Multi-function devices	Printers, copy machines, etc.
Network and network related devices and systems	Routers, switches, access points, etc.
Operating systems	Operating systems for various use cases
Other devices and systems	IoT products, medical devices and systems, ICS products, smart meters, etc.
Products for digital signatures	Secure signature tools
Trusted computing	Roots of trust, secure firmware, etc.

Common Criteria Evaluation

The main process steps related to a CC evaluation, as well as the involved stakeholders are summarized in the diagram below. The stakeholders of the scheme are RDI and TrustCB as a Certification Body.



Evaluation Process
Bureau Veritas works with manufacturers throughout the Common Criteria evaluation process, from Security Target review to documentation assessment, technical testing and reporting.

Security Target
Before evaluation starts, a Security Target (ST) defines the evaluation scope, security functionality and security claims to be verified. A well-defined ST helps reduce delays and rework during certification.

Evaluation Assurance Levels

Common Criteria evaluations can be performed at different Evaluation Assurance Levels (EALs), ranging from EAL1 to EAL7. Higher assurance levels require more extensive evaluation activities, documentation review and testing. EUCC evaluations can also be performed, with assurance levels including Substantial and High.

Evaluation Objectives

- Verify that the product meets the security requirements defined in the Security Target
- Assess the effectiveness of the product's security functionality
- Review the completeness and accuracy of product documentation
- Assess the security of the product development lifecycle

Typical Evaluation Activities

- Security Target review
- Product documentation assessment
- Product guidance review
- Vulnerability analysis and penetration testing
- Evaluation Technical Report (ETR)

Certification Outcome
At the end of the evaluation, Bureau Veritas Cybersecurity delivers the Evaluation Technical Report (ETR) to the certification body under the CC Scheme. The ETR forms the basis for the Certificate of Conformity for your product.

Your Partner for Common Criteria Certification

Bureau Veritas Cybersecurity supports manufacturers and developers throughout the Common Criteria certification journey. From initial preparation and Security Target development to evaluation activities and certification support, our experts help organizations achieve certification efficiently while reducing evaluation risks and unnecessary rework.

Our Common Criteria services include:

- Guidance on certification scope and strategy
- Support with Security Target and documentation preparation
- Documentation review and gap identification
- Vulnerability assessment and penetration testing
- Formal Common Criteria evaluation activities
- Certification support under the Dutch CC scheme

By combining deep technical expertise with extensive certification experience, we help organizations reduce evaluation risks, avoid unnecessary rework and achieve certification more efficiently.

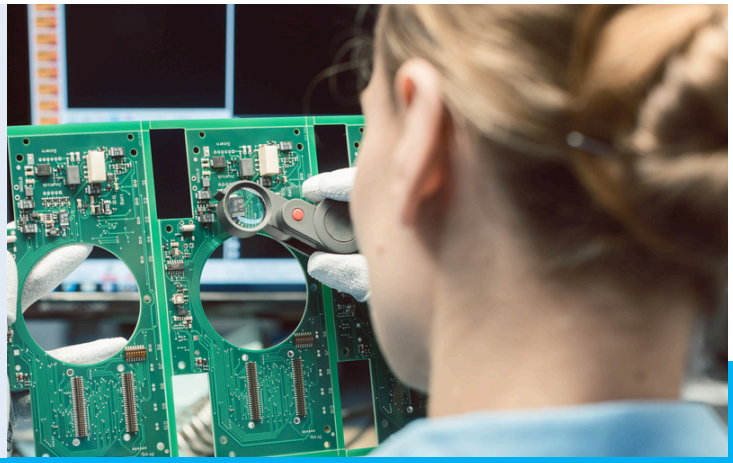
Why choose Bureau Veritas

Bureau Veritas Cybersecurity is your expert partner in cybersecurity. We help organizations identify risks, strengthen defenses and comply with cybersecurity standards and regulations. Our services cover people, processes and technology, ranging from awareness training and social engineering to security advice, compliance and penetration testing.

We operate across IT, OT and IoT environments, supporting both digital systems and connected products. With over 300 cybersecurity professionals worldwide, we combine deep technical expertise with a global presence. Bureau Veritas Cybersecurity is part of the Bureau Veritas Group, a global leader in testing, inspection and certification.

Planning a Common Criteria Certification Project?

Speak with our experts to discuss certification requirements, evaluation scope and the most suitable certification approach for your product.



cybersecurity@bureauveritas.com

cybersecurity.bureauveritas.com