SmartSuite

Framework / Cybersecurity / Other

Common Criteria for Information Technology Security Evaluation (CC:2022)

The Common Criteria (CC:2022, ISO/IEC 15408) is the international standard for specifying and independently evaluating the security of IT products.

What it is

The Common Criteria for Information Technology Security Evaluation (CC) is the international standard for specifying and independently evaluating the security of IT products, and CC:2022 Revision 1, published in November 2022, is its current edition. It gives buyers, developers and evaluators a common language for security functional requirements and security assurance requirements, so that the result of one evaluation can be compared with another and reused across borders.

At a glance

PUBLISHER
Common Criteria Recognition Arrangement (CCRA) participants, jointly with ISO/IEC

TYPE
Standard

VERSION
CC:2022 Revision 1

EFFECTIVE
November 2022

DOMAIN
Cybersecurity

FAMILY
Other

REGION
International (CCRA member nations)

INDUSTRY
Government & Public Sector

ADOPTION MODEL
Certification

IMPLEMENTATION COMPLEXITY
High

Source: commoncriteriaportal.org/cc/index.cfm

Why it matters

- **One evaluation, recognized in many countries** Certificates issued by an authorizing scheme are recognized by all signatories of the CCRA, which lists 18 authorizing and 18 consuming members on the CC Portal.
- **A shared vocabulary for security claims** Security functional requirements in Part 2 and security assurance requirements in Part 3 let a vendor state exactly what the product does and how deeply it was checked.
- **Graded assurance** Part 5 defines seven evaluation assurance levels, from EAL1 (functionally tested) to EAL7 (formally verified design and tested), plus composed assurance packages for products built from certified parts.
- **Comparable results from licensed laboratories** Evaluations are performed by competent, independent licensed laboratories using the common evaluation methodology, so results from different countries follow the same method.

Updated Nov 10, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports Common Criteria (ISO/IEC 15408)

Security Target Requirements Library

Record the security functional and assurance requirements each product claims, linked to the Protection Profile it conforms to.

Ownership, Cadence, and Accountability

Assign an owner to each evaluation workstream and set review dates for evidence, guidance documents and assurance continuity tasks.

Evidence Collection and Audit Trail

Keep design documents, test results and laboratory observation reports linked to the requirement they support, with dates and reviewers.

Testing and Vulnerability Findings

Track developer tests, laboratory findings and vulnerability analysis items through to closure before certification.

Supplier Certificate Tracking

Record the CC certificates, assurance packages and certificate dates of the third-party products your own systems rely on.

Certification Status Reporting

Report which products are in evaluation, certified, under maintenance or due for re-evaluation across schemes.

Common framework mappings

FIPS 140-3 · EU CRA · IEC 62443-4-2 · ISO 27001:2022

Official resources

CC:2022 and CEM:2022 publications

The Common Criteria Portal page with the five parts of CC:2022, CEM:2022, errata and supporting documents.

commoncriteriaportal.org/cc/index.cfm

Transition Policy to CC:2022 and CEM:2022

CCRA Management Committee policy CCMC-2023-04-001 setting the dates for moving from CC v3.1 to CC:2022.

commoncriteriaportal.org/files/ccfiles/CC2022CEM2022TransitionPolicy.pdf

Members of the CCRA

The certificate authorizing and certificate consuming members of the Common Criteria Recognition Arrangement.

commoncriteriaportal.org/ccra/members/index.cfm

Common Criteria certified products

The CC Portal list of certified products with their Security Targets and certification reports.

commoncriteriaportal.org/products/index.cfm

Frequently asked questions

What is the Common Criteria (ISO/IEC 15408)?

The Common Criteria for Information Technology Security Evaluation is the international standard for specifying and evaluating the security of IT products. Its current edition, CC:2022 Revision 1, was published in November 2022, and the same text is published by ISO/IEC as ISO/IEC 15408-1:2022 to 15408-5:2022.

Who publishes the Common Criteria?

CC:2022 was developed first as ISO/IEC standards and then published by the participants of the Common Criteria Recognition Arrangement (CCRA) on the Common Criteria Portal. The governmental organizations listed in its legal notice hold the copyright jointly with ISO/IEC and make the CC parts available for download.

What are the Common Criteria evaluation assurance levels?

CC:2022 Part 5 defines seven evaluation assurance levels: EAL1 functionally tested, EAL2 structurally tested, EAL3 methodically tested and checked, EAL4 methodically designed, tested and reviewed, EAL5 semi-formally verified designed and tested, EAL6 semi-formally verified design and tested, and EAL7 formally verified design and tested. Many evaluations today claim conformance to a Protection Profile instead of, or as well as, an EAL.

Updated Nov 10, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What is the difference between a Protection Profile and a Security Target?

A Protection Profile states the security needs for a type of product, independent of any one implementation. A Security Target states the security claims for one specific product, is the document the evaluation is performed against, and may claim conformance to one or more Protection Profiles.

Is CC v3.1 Revision 5 still valid?

CC v3.1 Revision 5 is the last revision of version 3.1 and could optionally be used for evaluations starting no later than June 30, 2024. Under the CCRA transition policy, Security Targets conformant to CC:2022 that are based on Protection Profiles certified under CC v3.1 are accepted up to December 31, 2027, and re-evaluations based on CC v3.1 evaluations can be started for up to two years from the initial certification date.

How many countries recognize Common Criteria certificates?

The CC Portal lists 36 members of the Common Criteria Recognition Arrangement: 18 certificate authorizing members, which run national certification schemes, and 18 certificate consuming members, which recognize certificates without issuing their own. Certificates issued under the arrangement are recognized by all signatories.

Is Common Criteria certification a requirement for SaaS providers?

The Common Criteria evaluates IT products in a defined configuration, not an organization's operations, so it is not a general requirement for software-as-a-service providers. It applies where a government buyer or procurement rule asks for an evaluated product, and SaaS providers more often answer operational security questions with reports and certifications such as ISO/IEC 27001.

License included / downloadable: Yes CC:2022 Parts 1 to 5 and CEM:2022 are free to download from the Common Criteria Portal, where the governmental copyright holders grant users the right to reuse their text; the ISO/IEC 15408 and 18045 editions are sold by ISO and are not included.

Full framework page and mappings: smartsuite.com/frameworks/common-criteria-iso-iec-15408-cc-2022-it-security-evaluation