Cyber Security – Common Criteria Standards Package

Common Criteria (CC) is an international set of guidelines and specifications developed for evaluating information security products, specifically to ensure they meet an agreed-upon security standard for government deployments.

To order this standards package, click here

INCITS/ISO/IEC 15408-1:2009[R2017]
Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model

This standard establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of ISO/IEC 15408; defines the terms and abbreviations to be used in all parts ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations.
The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified, and the consequences of evaluation and evaluation results are described.

INCITS/ISO/IEC 15408-2:2008[R2018]
Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components

This standard defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will meet most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes.

ISO/IEC 15408-2:2008 also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist.

INCITS/ISO/IEC 15408-3:2008[R2018]
Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components

This standard defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component targets of evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets.

ISO/IEC 15408-3:2008 defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organization of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.

INCITS/ISO/IEC 18045:2008[R2018]
Information technology — Security techniques — Methodology for IT security evaluation

This standard is a companion document to ISO/IEC 15408,*Information technology - Security techniques - Evaluation criteria for IT security*. ISO/IEC 18045:2008 defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408. ISO/IEC 18045:2008 does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

INCITS/Cyber Security Technical Committee

The INCITS/Cyber Security area of work addresses standardization in the areas assigned to ISO/IEC JTC 1/SC 27 which include:

The scope of Technical Committee INCITS/CS1 on Cyber Security is focused on the development of international standards in information security, cybersecurity, and privacy protection. This includes generic methods, techniques, and guidelines to address both security and privacy aspects, such as:

- Management of cybersecurity; in particular, information security management system (ISMS) standards, security processes, security controls and services.
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity, and confidentiality of information.
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components.
- Security aspects of identity management, biometrics, and privacy.
- Conformance assessment, accreditation, and auditing requirements in the area of information security management systems.
- Security evaluation criteria and methodology and security requirements for cryptographic modules.
- Security requirements capture methodology.

The scope of CS1 also includes the development of U.S. standards in information security, cybersecurity, and privacy protection. Additionally, CS1 can collaborate with other INCITS technical committee to ensure that security and privacy are adequately addressed in U.S. standards that do not have information security, cybersecurity, and privacy protection as a primary focus.

The scope of CS1 explicitly excludes the areas of work on cyber security standardization presently underway in INCITS B10, M1, T3, T10 and T11 as well as other standard groups, such as ATIS, IEEE, IETF, TIA, and X9.

To learn more about the activities of the technical committee and how to participate in the development of these and other deliverables, please contact INCITS.
