INTERNATIONAL STANDARD

ISO/IEC 15408-3

Fourth edition
2022-08

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 3: Security assurance components

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information —

Partie 3: Composants d'assurance de sécurité

Reference number
ISO/IEC 15408-3:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 15408-3:2008), which has been technically revised.

The main changes are as follows:

— the terminology has been reviewed and updated;

— the exact conformance type has been incorporated;

— low assurance PPs have been removed and direct rationale PPs have been incorporated;

— PP-Modules and PP-Configurations for modular evaluations have been incorporated;

— multi-assurance evaluation has been incorporated.

A list of all parts in the ISO/IEC 15408 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations (called CC), they hereby grant non-exclusive license to ISO/IEC to use CC in the continued development/maintenance of the ISO/IEC 15408 series of standards. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC as they see fit.

Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale de la Sécurité des Systèmes d'Information
Germany	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Netherlands	Netherlands National Communications Security Agency
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Ministerio de Asuntos Económicos y Transformación Digital
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency

Introduction

Security assurance components, as defined in this document, are the basis for the security assurance requirements expressed in a Security Assurance Package, Protection Profile (PP), a PP-Module, a PP-Configuration, or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This document catalogues the set of assurance components, families and classes. It also defines evaluation criteria for PPs, PP-Configurations, PP-Modules, and STs.

The audience for this document includes consumers, developers, technical working groups, evaluators of secure IT products and others. ISO/IEC 15408-1:2022, Clause 5 provides additional information on the target audience of the ISO/IEC 15408 series, and on the use of the ISO/IEC 15408 series by the groups that comprise the target audience. These groups may use this document as follows:

a) Consumers, who use this document when selecting components to express assurance requirements to satisfy the security objectives expressed in a PP or ST, determining required levels of security assurance of the TOE.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this document when interpreting statements of assurance requirements and determining assurance approaches of TOEs.

c) Evaluators, who use the assurance requirements defined in this document as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —

Part 3: Security assurance components

1 Scope

This document defines the assurance requirements of the ISO/IEC 15408 series. It includes the individual assurance components from which the evaluation assurance levels and other packages contained in ISO/IEC 15408-5 are composed, and the criteria for evaluation of Protection Profiles (PPs), PP-Configurations, PP-Modules, and Security Targets (STs).

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1:2022, *Information security — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information security — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-4, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 15408-5, *Information security — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

ISO/IEC 18045:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation*

ISO/IEC IEEE 24765, *Systems and software engineering — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-4, ISO/IEC 15408-5, ISO/IEC 18045 and ISO/IEC IEEE 24765 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
acceptance procedure
procedure followed in order to accept newly created or modified *configuration items* (3.3) as part of the target of evaluation (TOE), or to move them to the next step of the life-cycle

Note 1 to entry: These procedures identify the roles or individuals responsible for the acceptance and the criteria to be applied in order to decide on the acceptance.

Note 2 to entry: There are several types of acceptance situations some of which can overlap:

a) acceptance of an item into the configuration management system for the first time, in particular as part of an integration process;

b) progression of configuration items to the next life-cycle phase at each stage of the construction of the TOE

EXAMPLE 1 Module, subsystem, quality control of the finished TOE;

c) subsequent to transport of configuration items

EXAMPLE 2 Parts of the TOE or preliminary products between different *development* (3.15) sites;

d) subsequent to the *delivery* (3.14) of the TOE to the consumer;

e) subsequent to the integration of the TOE

EXAMPLE 3 Inclusion of software, firmware and hardware components from other sources into the TOE.

3.2
action
evaluator or developer action element of ISO/IEC 15408-3

Note 1 to entry: These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.

3.3
configuration item
item or aggregation of hardware, software, or both that is designated for configuration management and treated as a single entity in the configuration management process, during the target of evaluation (TOE) *development* (3.15)

Note 1 to entry: These can be either parts of the TOE or objects related to the development of the TOE, e.g. evaluation documents or development tools. Configuration management items can be stored in the configuration management system directly (for example, files) or by reference (for example, hardware parts) together with their version.

3.4
configuration list
configuration management output (3.8) document listing all *configuration items* (3.3) for a specific product together with the exact version of each configuration management item relevant for a specific version of the complete product

Note 1 to entry: This list allows distinguishing the items belonging to the evaluated version of the product from other versions of these items belonging to other versions of the product. The final configuration management list is a specific document for a specific version of a specific product. (Of course, the list can be an electronic document inside of a *configuration management tool* (3.12). In that case, it can be seen as a specific view into the system or a part of the system rather than an output of the system. However, for the practical use in an evaluation the configuration list will probably be delivered as a part of the evaluation documentation.) The configuration list defines the items that are under the configuration management requirements of ALC_CMC.

3.5
configuration management
CM
discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a *configuration item* (3.3), control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements

[SOURCE: ISO/IEC IEEE 24765:2017, 3.779 1]

3.6
configuration management documentation
CM documentation
documentation including *configuration management output* (3.8), configuration management list(s), *configuration management system records* (3.11), *configuration management plan* (3.9) and *configuration management usage documentation* (3.13)

3.7
configuration management evidence
everything that may be used to establish confidence in the correct operation of the configuration management system

EXAMPLE *Configuration management output* (3.8), rationales provided by the developer, observations, experiments, or interviews made by the evaluator during a site visit.

3.8
configuration management output
results, related to configuration management, produced, or enforced by the configuration management system

Note 1 to entry: These configuration management related results can occur as documents (e.g. filled paper forms, *configuration management system records* (3.11), logging data, hard-copies, and electronic output data) as well as actions (e.g. manual measures to fulfil configuration management instructions). Examples of such configuration management outputs are *configuration lists* (3.4), *configuration management plans* (3.9) and/or behaviours during the product life-cycle.

3.9
configuration management plan
description of how the configuration management system is used for the target of evaluation (TOE)

Note 1 to entry: The objective of issuing a configuration management plan is that staff members can see clearly what they have to do. From the point of view of the overall configuration management system this can be seen as an output document (because it can be produced as part of the application of the configuration management system). From the point of view of the concrete project it is a usage document because members of the project team use it in order to understand the steps that they have to perform during the project. The configuration management plan defines the usage of the system for the specific product; the same system can be used to a different extent for other products. The configuration management plan defines and describes the output of the configuration management system of a company which is used during the TOE *development* (3.15).

EXAMPLE The structure and content of a configuration management plan are presented in ISO 10007:2017, Annex A.

3.10
configuration management system
set of procedures and tools (including their documentation) used by a developer to develop and maintain configurations of their products during their life-cycles

Note 1 to entry: Configuration management systems can have varying degrees of rigour and function. At higher levels, configuration management systems can be automated, with flaw remediation, change controls, and other tracking mechanisms.

3.11
configuration management system record
output produced during the operation of the configuration management system documenting important configuration management activities

EXAMPLE Configuration management item change control forms and configuration management item access approval forms.