International Standard

ISO/IEC 15408-1

Fifth edition
2026-05

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

Part 1: Introduction and general model

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

Partie 1: Introduction et modèle général

Reference number
ISO/IEC 15408-1:2026(en)

COPYRIGHT PROTECTED DOCUMENT

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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This fifth edition cancels and replaces the fourth edition (ISO/IEC 15408-1:2022), which has been technically revised.

The main changes are as follows:

— the terminology has been reviewed and updated;

— the package conformance claim for Security Targets, Protection Profiles and PP-Modules, respectively, has been reviewed and aligned with ISO/IEC 18045;

— the specification of multiple PP-Modules Bases has been improved for accuracy;

— corrections of mistakes.

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

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.

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware, or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance applied to these IT products meet relevant requirements.

The evaluation results can help consumers to determine whether these IT products fulfil their security needs.

The ISO/IEC 15408 series is useful as a guide for the development, evaluation or procurement of IT products with security functionality.

The ISO/IEC 15408 series is intentionally flexible, enabling a range of evaluation approaches to be applied to a range of security properties of a range of IT products. Therefore, users of this document are recommended to ensure that this flexibility is not misused. For example, using the ISO/IEC 15408 series in conjunction with unsuitable evaluation methods/activities, irrelevant security properties, or inappropriate IT products, can result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties, and methods to determine that an evaluation provides meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

The ISO/IEC 15408 series addresses the protection of assets from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity and availability. The ISO/IEC 15408 series can also be applicable to aspects of IT security outside of these three categories. The ISO/IEC 15408 series is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. The ISO/IEC 15408 series may be applied in other areas of IT but makes no claim of applicability in these areas.

The ISO/IEC 15408 series is presented as a set of distinct but related parts as identified below.

a) ISO/IEC 15408-1 is the introduction to the ISO/IEC 15408 series. It defines the general concepts and principles of IT security evaluation and presents a general model of evaluation.

b) ISO/IEC 15408-2 establishes a set of functional components that serve as standard templates upon which security functional requirements (SFRs) for Target of Evaluations (TOEs) are based. ISO/IEC 15408-2 catalogues the set of security functional components and organizes them into families and classes.

c) ISO/IEC 15408-3 establishes a set of assurance components that serve as standard templates upon which security assurance requirements for TOEs are based. ISO/IEC 15408-3 catalogues the set of security assurance components and organizes them into families and classes. ISO/IEC 15408-3 also defines evaluation criteria for PPs, STs and TOEs.

d) ISO/IEC 15408-4 provides a standardized framework for the specification of evaluation methods and activities that may be included in PPs, STs and any documents supporting them, to be used by evaluators in support of evaluations using the model described in the other parts of the ISO/IEC 15408 series. ISO/IEC 18045 is fundamental to ISO/IEC 15408-4.

e) ISO/IEC 15408-5 provides packages of security assurance and SFRs that have been identified as useful in support of common usage by stakeholders. Examples of provided packages include the evaluation assurance levels (EAL) and the composed assurance packages (CAPs).

NOTE 1 ISO/IEC 18045 provides the baseline methodology for IT security evaluations performed in accordance with the ISO/IEC 15408 series.

Certain topics, which involve specialized techniques or are somewhat peripheral to IT security, are considered to be outside the scope of the ISO/IEC 15408 series. The following list of topics are not covered by the ISO/IEC 15408 series:

f) security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognized that significant security can often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls;

g) the evaluation methodology under which the criteria should be applied;

NOTE 2 The baseline methodology is defined in ISO/IEC 18045. ISO/IEC 15408-4 can be used to further derive evaluation activities and methods from ISO/IEC 18045.

h) administrative and legal framework under which the criteria can be applied by evaluation authorities. However, it is expected that the ISO/IEC 15408 series is intended to be used for evaluation purposes in the context of such a framework;

i) the procedures for use of evaluation results in accreditation. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors shall make separate provisions for those aspects;

j) the subject of criteria for the assessment of the inherent qualities of cryptographic algorithms. In the case that independent assessment of mathematical properties of cryptography is required, the evaluation scheme under which the ISO/IEC 15408 series is applied can make provision for such assessments.

This document introduces:

— the key concepts of Protection Profiles (PP), PP-Modules, PP-Configurations, packages, Security Targets (ST), and conformance types;

— a description of the organization of security components throughout the model;

— the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be tailored through the use of permitted operations;

— general information about the evaluation methods given in ISO/IEC 18045;

— guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045;

— general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5;

— information regarding the scope of evaluation schemes.

The following text appears in other parts of the ISO/IEC 15408 series and in ISO/IEC 18045 to describe the use of bold and italic type in those documents. This document may use those conventions only in examples, but the notes have been retained for alignment with the rest of the series.

Bold type is used to highlight hierarchical relationships between requirements. This convention calls for the use of bold type for all new requirements.

For security functional requirements, the use of italics denotes assignment and selection items.

For security assurance requirements, special verbs relating to mandatory evaluation activities are presented in bold italic type face.

Several governmental organizations have 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. More information on these agencies can be found at https://commoncriteriaportal.org/cc/copyright/index.cfm.

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

Part 1: Introduction and general model

1 Scope

This document establishes the general concepts and principles of information technology (IT) security evaluation. It specifies the general model of evaluation given in this document, which in its entirety is intended to be used as the basis for evaluation of security properties of IT products.

This document provides an overview of all parts of the ISO/IEC 15408 series. It describes the various parts of the ISO/IEC 15408 series i.e.

— defines the terms and abbreviations used in all parts of the series; establishes the core concept of a Target of Evaluation (TOE);

— describes the evaluation context; and

— describes the audience to which the evaluation criteria is addressed.

Additionally, this document introduces the basic security concepts necessary for the evaluation of IT products.

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 15408-2:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

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

ISO/IEC IEEE 24765:2017, *Systems and software engineering — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-2, ISO/IEC 15408-3, 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
action
documented activity of the *evaluator* (3.46) or *developer* (3.34)

Note 1 to entry: Evaluator actions and developer actions are required by ISO/IEC 15408-3.

3.2
administrator
entity (3.37) that has a level of trust with respect to all policies implemented by the *TOE security functionality (TSF)* (3.95)

Note 1 to entry: Not all *Protection Profiles (PPs)* (3.71) or *Security Targets (STs)* (3.85) assume the same level of trust for administrators. Typically, administrators are assumed to adhere at all times to the policies in the ST of the *target of evaluation (TOE)* (3.93). Some of these policies can be related to the functionality of the TOE, while others can be related to the *operational environment* (3.66).

3.3
adverse action
action (3.1) performed by a *threat agent* (3.94) on an *asset* (3.5)

3.4
allowed-with
statement that relates to exact conformance and states which other *PPs* (3.71) and *PP-Modules* (3.74) are permitted to be included in a conformance claim with the *PP* (3.71) or *PP-Module* (3.74) or *PP-Configuration* (3.72) with a given *PP-Module* (3.74)

3.5
asset
entity (3.37) that the owner of the *target of evaluation (TOE)* (3.93) presumably places value on

3.6
assignment
specification of an identified parameter in a functional or assurance component

3.7
assurance
grounds for confidence that a *target of evaluation (TOE)* (3.93) meets the *security functional requirements (SFRs)* (3.81)

3.8
assurance package
named set of *security assurance requirements* (3.79)

EXAMPLE EAL3.

3.9
attack potential
measure of the effort needed to exploit a vulnerability in a *target of evaluation (TOE)* (3.93)

Note 1 to entry: The effort is expressed as a function of properties related to the attacker (e.g. expertise, resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure).

3.10
attack surface
set of logical or physical interfaces to a target, consisting of points through which access to the target and its functions can be attempted

EXAMPLE 1 The casing of a payment terminal is a part of physical attack surface for that device.

EXAMPLE 2 The communications protocols available for connection to a network device are part of the logical attack surface for that network device.

3.11
augmentation
addition of one or more requirements to a package

Note 1 to entry: In case of a *functional package* (3.51), such an augmentation is considered only in the context of one package and is not considered in the context with other packages or *Protection Profiles (PPs)* (3.71) or *Security Targets (STs)* (3.85).

Note 2 to entry: In case of an *assurance package* (3.8), augmentation refers to one or more *security assurance requirements (SARs)* (3.79).

3.12
authorized user
entity (3.37) who is allowed, in accordance with the *security functional requirements (SFRs)* (3.81), to perform an operation on the *target of evaluation (TOE)* (3.93)

3.13
base component
independent *entity* (3.37) in a multi-component product that provides services and resources to one or more *dependent component(s)* (3.32)

Note 1 to entry: This applies in particular to *composed TOEs* (3.22) and composite products/*composite TOEs* (3.26).

3.14
base Protection Profile
base PP
Protection Profile (3.71) specified in a *PP-Module Base* (3.75) which is used to build a *PP-Configuration* (3.72)

3.15
base PP-Module
PP-Module (3.74) specified in a *PP-Module Base* (3.75) which is used to build a *PP-Configuration* (3.72)

Note 1 to entry: Specifying a base PP-Module in a *PP-Module* (3.74) implicitly includes the base PP-Module's PP-Module Base.

3.16
base target of evaluation
base TOE
base component (3.13) which is itself the subject of an evaluation

Note 1 to entry: This applies in particular to *composed TOEs* (3.22) and composite products/*composite TOEs* (3.26).

3.17
class
⟨taxonomy⟩ set of families that share a common focus

Note 1 to entry: Class is further defined in ISO/IEC 15408-2, which defines security functional classes, and ISO/IEC 15408-3, which defines security assurance classes.

3.18
component
⟨taxonomy⟩ smallest selectable set of elements on which requirements can be based

3.19
component
⟨composition⟩ *entity* (3.37) which provides resources and services in a product

3.20
component target of evaluation
component TOE
target of evaluation (TOE) (3.93) that is a component of a *composed TOE* (3.22)

Note 1 to entry: A component TOE is usually evaluated before the evaluation of the composed TOE.

3.21
composed assurance package
CAP
assurance package (3.8) consisting of components drawn predominately from the composition assurance (ACO) *class* (3.17), representing a point on the pre-defined scale for composition assurance

3.22
composed target of evaluation
composed TOE
target of evaluation (TOE) (3.93) comprising solely two or more separately identified components with a security relationship between their *TOE security functionality (TSFs)* (3.95)

Note 1 to entry: Each of the separately identified components is itself a TOE.

3.23
composed evaluation
evaluation of a *composed target of evaluation* (3.22) using the specific evaluation technique applicable to composed TOEs

Note 1 to entry: This evaluation technique refers to the composition assurance (ACO) *class* (3.17) that is defined in ISO/IEC 15408-3.

3.24
composite evaluation
evaluation of a *composite target of evaluation/product* (3.26) using the specific composite evaluation technique

Note 1 to entry: This evaluation technique refers to the composite related assurance families (COMP) that are specified in ISO/IEC 15408-3:2026 for the ADV, ALC, ASE, ATE and AVA assurance *classes* (3.17).

3.25
composite product
product comprised of two or more components which can be organized in two layers: a layer of one already evaluated *base component* (3.13) (*base target of evaluation* (3.16)) and a layer of one *dependent component* (3.32)

3.26
composite target of evaluation
composite TOE
part of a *composite product* (3.25) including the *base target of evaluation (TOE)* (3.16) and the *dependent component* (3.32)

Note 1 to entry: A dependent component in a composite TOE can consist of one or more dependent components. For simplification, they are considered as one dependent component.

Note 2 to entry: A composite TOE can contain parts that are independent from the *base component* (3.13) or base TOE respectively. For simplification, such parts are considered as belonging to the dependent component.

Note 3 to entry: The *composite evaluation* (3.24) can be applied as many times as necessary to a multi-component/ multi-layered product, in an incremental approach.

3.27
configuration management
CM
discipline applying technical and administrative direction and surveillance to identify and document the functional and physical characteristics of a configuration item, 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, modified — definitions 2 and 3 have been removed.]

3.28
configuration management system
set of procedures and tools (including their documentation) used by a *developer* (3.34) 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.

3.29
counter, verb
act on or respond to a particular threat so that the threat is eradicated or mitigated

3.30
demonstrable conformance
relation between a *Protection Profile (PP)* (3.71)/ *Security Target (ST)* (3.85) and a PP, or an ST and a *PP-Configuration* (3.72), where the PP/ST provides an equivalent or more restrictive solution that solves the generic security problem in the PP/PP-Configuration

3.31
dependency
relationship between components such that a *Protection Profile (PP)* (3.71), *Security Target (ST)* (3.85), *PP-Module* (3.74), *functional package* (3.52) or *assurance package* (3.8) including a component also includes any other components that are depended upon or otherwise provides a rationale for discarding such dependency

3.32
dependent component
dependent *entity* (3.37) in a multi-component product that relies on the provision of services and resources by one or more *base components* (3.13)

Note 1 to entry: This applies in particular to *composed target of evaluations (TOEs)* (3.22) and composite products/ *composite TOEs* (3.26).

3.33
dependent target of evaluation
dependent TOE
dependent component (3.32) which is itself the subject of an evaluation

Note 1 to entry: This applies only to *composed target of evaluations (TOEs)* (3.22) and not to composite products/ *composite TOEs* (3.26).

3.34
developer
organization responsible for the development of the *target of evaluation (TOE)* (3.93)

3.35
direct rationale
type of *Protection Profile* (3.71), *PP-Module* (3.74) or *Security Target* (3.85) in which the *security problem definition (SPD)* (3.83) elements are mapped directly to the *security functional requirements (SFRs)* (3.81) and possibly to the *security objectives* (3.82) for the *operational environment* (3.66)

Note 1 to entry: Direct rationale does not include security objectives for the *target of evaluation (TOE)* (3.93).

3.36
element
⟨taxonomy⟩ self-contained description of a security need assigned to *security assurance requirement (SAR)* (3.79) or *security functional requirement (SFR)* (3.81)