International

ISO/IEC 15408-1

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

Fifth edition
2026-05

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

Foreword ... **vi**
Introduction ... **vii**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **13**
5 Overview ... **14**
5.1 General ... 14
5.2 ISO/IEC 15408 series audience ... 14
5.2.1 General ... 14
5.2.2 Consumers (Risk owners) ... 14
5.2.3 Developers ... 14
5.2.4 Technical working groups ... 15
5.2.5 Evaluators ... 15
5.2.6 Others ... 15
5.3 Target of evaluation (TOE) ... 17
5.3.1 General ... 17
5.3.2 TOE boundaries ... 18
5.3.3 Different representations of the TOE ... 18
5.3.4 Different configurations of the TOE ... 18
5.3.5 Operational environment of the TOE ... 19
5.4 Presentation of material in this document ... 19
6 General model ... **19**
6.1 Background ... 19
6.2 Assets and security controls ... 20
6.3 Core constructs of the paradigm of the ISO/IEC 15408 series ... 22
6.3.1 General ... 22
6.3.2 Conformance types ... 23
6.3.3 Communicating security requirements ... 23
6.3.4 Meeting the needs of consumers (risk owners) ... 26
7 Specifying security requirements ... **27**
7.1 Security problem definition (SPD) ... 27
7.1.1 General ... 27
7.1.2 Threats ... 27
7.1.3 Organizational security policies (OSPs) ... 28
7.1.4 Assumptions ... 28
7.2 Security objectives ... 29
7.2.1 General ... 29
7.2.2 Security objectives for the TOE ... 29
7.2.3 Security objectives for the operational environment ... 29
7.2.4 Relation between security objectives and the SPD ... 30
7.2.5 Tracing between security objectives and the SPD ... 30
7.2.6 Providing a justification for the tracing ... 31
7.2.7 On countering threats ... 31
7.2.8 Security objectives: conclusion ... 31
7.3 Security requirements ... 31
7.3.1 General ... 31
7.3.2 Security Functional Requirements (SFRs) ... 32
7.3.3 Security assurance requirements (SARs) ... 34
7.3.4 Security requirements: conclusion ... 35
8 Security components ... **36**
8.1 Hierarchical structure of security components ... 36

8.1.3 Family 36
8.1.4 Component 36
8.1.5 Element 36
8.2 Operations 37
8.2.1 General 37
8.2.2 Iteration 37
8.2.3 Assignment 38
8.2.4 Selection 39
8.2.5 Refinement 40
8.3 Dependencies between components 41
8.4 Extended components 42
8.4.1 General 42
8.4.2 Defining extended components 42

9 Packages 43
9.1 General 43
9.2 Package types 44
9.2.1 General 44
9.2.2 Assurance packages 44
9.2.3 Functional packages 44
9.3 Package dependencies 45
9.4 Evaluation method(s) and activities 45

10 Protection Profiles (PPs) 45
10.1 General 45
10.2 PP introduction 46
10.3 Conformance claims and conformance statements 46
10.4 Security assurance requirements (SARs) 48
10.5 Additional requirements common to strict and demonstrable conformance 49
10.5.1 Conformance claims and conformance statements 49
10.5.2 Security problem definition (SPD) 49
10.5.3 Security objectives 49
10.6 Additional requirements specific to strict conformance 49
10.6.1 Requirements for the security problem definition (SPD) 49
10.6.2 Requirements for the security objectives 50
10.6.3 Requirements for the security requirements 50
10.7 Additional requirements specific to demonstrable conformance 50
10.8 Additional requirements specific to exact conformance 50
10.8.1 General 50
10.8.2 Conformance claims and conformance statements 51
10.9 Using PPs 51
10.10 Conformance statements and claims in the case of multiple PPs 52
10.10.1 General 52
10.10.2 Where strict or demonstrable conformance is specified 52
10.10.3 Where exact conformance is specified 52

11 Modular requirements construction 52
11.1 General 52
11.2 PP-Modules 52
11.2.1 General 52
11.2.2 PP-Module Base 53
11.2.3 Requirements for PP-Modules 53
11.3 PP-Configurations 56
11.3.1 General 56
11.3.2 Requirements for PP-Configurations 57
11.3.3 Usage of PP-Configurations 62

12 Security Targets (STs) 65
12.1 General 65

12.4 Additional requirements in the exact conformance case ... 69
12.4.1 Additional requirements for the conformance claim ... 69
12.4.2 Additional requirements for the SPD ... 69
12.4.3 Additional requirements for the security objectives ... 69
12.4.4 Additional requirements for the security requirements ... 69
12.5 Additional requirements in the multi-assurance case ... 70

13 Evaluation and evaluation results ... 71
13.1 General ... 71
13.2 Evaluation context ... 73
13.3 Evaluation of PPs and PP-Configurations ... 73
13.4 Evaluation of STs ... 74
13.5 Evaluation of TOEs ... 74
13.6 Evaluation methods and evaluation activities ... 75
13.7 Evaluation results ... 75
13.7.1 Results of a PP evaluation ... 75
13.7.2 Results of a PP-Configuration evaluation ... 75
13.7.3 Results of an ST/TOE evaluation ... 75
13.8 Multi-assurance evaluation ... 76

14 Composition of assurance ... 77
14.1 General ... 77
14.2 Composition models ... 77
14.2.1 Layered composition model ... 77
14.2.2 Network or bi-directional composition model ... 78
14.2.3 Embedded composition model ... 79
14.3 Evaluation techniques for providing assurance in composition models ... 79
14.3.1 General ... 79
14.3.2 ACO class for composed TOEs ... 80
14.3.3 Composite evaluation for composite products ... 80
14.4 Requirements for evaluations using composition techniques ... 91
14.4.1 Re-use of evaluation results ... 91
14.4.2 Composition evaluation issues ... 92
14.5 Evaluation by composition and multi-assurance ... 93

Annex A (normative) **Specification of packages ... 94**

Annex B (normative) **Specification of Protection Profiles (PPs) ... 98**

Annex C (normative) **Specification of PP-Modules and PP-Configurations ... 107**

Annex D (normative) **Specification of Security Targets (STs) and direct rationale STs ... 121**

Annex E (normative) **PP/PP-Configuration conformance ... 132**

Bibliography ... 137

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.

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.

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

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.