International Standard

ISO/IEC 15408-2

Fifth edition
2026-05

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

Part 2: Security functional components

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

Partie 2: Composants fonctionnels de sécurité

Reference number
ISO/IEC 15408-2:2026(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 15408-2:2022), which has been technically revised.

The main changes are as follows:

— the document has been restructured;

— technical changes have been introduced:

  — the terminology has been reviewed and updated;

  — the dependency and hierarchy for each component have been reviewed and updated;

  — the new notes for operations have been introduced.

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

Security functional components, as defined in this document, are the basis for the security functional requirements (SFRs) or components expressed in a Protection Profile (PP), PP-Module, functional package or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP, PP-Module, functional package or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the Information Technology (IT) or by the IT response to stimulus.

Security functional components allow for the expression of SFRs intended to counter threats in the assumed operating environment of the TOE and cover any identified organizational security policies.

The audience for this document includes consumers, developers and evaluators of secure IT products. ISO/IEC 15408-1 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 use this document as follows:

— consumers, who use this document when selecting components to express functional requirements which satisfy the security objectives expressed in a PP, PP-Module, functional package or ST. ISO/IEC 15408-1 provides more detailed information on the relationship between security objectives and security requirements;

— developers, who respond to actual or perceived consumer security requirements in constructing a TOE and will find a standardized method to understand those requirements in this document. They also use the contents of this document as a basis for further defining the TOE security functionality and mechanisms that conform with those requirements;

— evaluators, who use the SFRs defined in this document in verifying that the TOE functional requirements expressed in the PP, PP-Module, functional package or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators use this document to assist in determining whether a given TOE satisfies stated requirements.

This document uses bold type 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.

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 2: Security functional components

1 Scope

This document specifies requirements for the required structure and content of security functional components for use during a security evaluation. It includes a catalogue of functional components that meet the common security functionality requirements of many 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 15408-1:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

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

ISO/IEC 18045:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Requirements and methodology for IT security evaluation*

Bibliography

[1] AIS 31, *Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren. Version 3, May 15,2020*

[2] ISO/IEC 9594-8, *Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks*

[3] ISO/IEC 15408-4:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

[4] ISO/IEC 15408-5:2026, *Information security — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

[5] ISO/IEC/TS 19249, *Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications*

[6] ISO/IEC/TS 19608, *Guidance for developing security and privacy functional requirements based on ISO/IEC 15408*

[7] ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*

[8] ITU-T Recommendation X.509, *Information technology – Open systems interconnection – The directory: Public-key and attribute certificate frameworks.*

[9] NIST SP 800-90A, *The National Institute of Standards and Technology (NIST). Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators, June 2015*

[10] NIST SP 800-90B, *The National Institute of Standards and Technology (NIST). Special Publication 800-90B Recommendation for the Entropy Sources Used for Random Bit Generation, January 2018*