International Standard

# ISO/IEC 15408-5

Second edition
2026-04

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

## Part 5: Pre-defined packages of security requirements

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

*Partie 5: Paquets prédéfinis d'exigences de sécurité*



Reference number
ISO/IEC 15408-5:2026(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 second edition cancels and replaces the first edition (ISO/IEC 15408-5:2022), which has been technically revised.

The main changes are as follows:

— the terminology has been reviewed and updated;

— mistakes have been corrected.

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

This document provides pre-defined packages of security requirements. Such security requirements can be useful for stakeholders as they strive for conformity between evaluations. Packages of security requirements can also help reduce the effort in developing Protection Profiles (PPs) and Security Targets (STs).

ISO/IEC 15408-1 defines the term “package” and describes the fundamental concepts concerning packages.

This document presents:

— evaluation assurance levels (EAL) (see Clause 4) family of packages that specify pre-defined sets of security assurance components that may be referenced in PPs and STs and which specify appropriate security assurances to be provided during an evaluation of a target of evaluation (TOE);

— composed assurance packages (CAP) (see Clause 5) family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during an evaluation of composed TOEs;

— composite product packages (COMP) (see Clause 6) family of packages that specifies a set of security assurance components used for specifying appropriate security assurances to be provided during an evaluation of a composite product TOEs;

— protection profile assurances (PPA) (see Clause 7) family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during a protection profile evaluation;

— security target assurances (STA) (see Clause 8) family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during a security target evaluation.



This document uses bold type to highlight hierarchical relationships between package objectives. This convention calls for the use of bold type for all new objectives.



Several governmental organizations have contributed to the development of this version of the Common Methodology for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Methodology for Information Technology Security Evaluations (called CEM), they hereby grant non-exclusive license to ISO/IEC to use CEM in the continued development/maintenance of the ISO/IEC 15408-5 International Standard. However, these governmental organizations retain the right to use, copy, distribute, translate, or modify CEM 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 5: Pre-defined packages of security requirements

## 1 Scope

This document provides packages of security assurance and security functional requirements that are intended to be useful in support of common usage by stakeholders.

The users of this document can include consumers, developers and evaluators of secure 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*



## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1 and ISO/IEC 15408-3 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.

## 4 Evaluation assurance levels (EAL)

### 4.1 Family name

The name of this family of packages is evaluation assurance levels (EALs).

### 4.2 Family overview

#### 4.2.1 General

The EALs provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The approach of ISO/IEC 15408-1 identifies the separate