



International
Standard

ISO/IEC 15408-5

**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

**Second edition
2026-04**

Sample Document

get full document from standards.iteh.ai



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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	vi
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Evaluation assurance levels (EAL)	1
4.1 Family name.....	1
4.2 Family overview.....	1
4.2.1 General.....	1
4.2.2 Relationship between assurances and assurance levels.....	2
4.3 Family objectives.....	4
4.4 Evaluation assurance level 1 (EAL1) — Functionally tested.....	5
4.4.1 Package name.....	5
4.4.2 Package type.....	5
4.4.3 Package overview.....	5
4.4.4 Package objectives.....	5
4.4.5 Package components.....	5
4.5 Evaluation assurance level 2 (EAL2) — Structurally tested.....	6
4.5.1 Package name.....	6
4.5.2 Package type.....	6
4.5.3 Package overview.....	6
4.5.4 Package objectives.....	6
4.5.5 Package components.....	7
4.6 Evaluation assurance level 3 (EAL3) — Methodically tested and checked.....	7
4.6.1 Package name.....	7
4.6.2 Package type.....	7
4.6.3 Package overview.....	7
4.6.4 Package objectives.....	8
4.6.5 Package components.....	8
4.7 Evaluation assurance level 4 (EAL4) — Methodically designed, tested and reviewed.....	9
4.7.1 Package name.....	9
4.7.2 Package type.....	9
4.7.3 Package overview.....	9
4.7.4 Package objectives.....	9
4.7.5 Package components.....	9
4.8 Evaluation assurance level 5 (EAL5) — Semi-formally designed and tested.....	10
4.8.1 Package name.....	10
4.8.2 Package type.....	10
4.8.3 Package overview.....	10
4.8.4 Package objectives.....	10
4.8.5 Package components.....	11
4.9 Evaluation assurance level 6 (EAL6) — Semi-formally verified design and tested.....	12
4.9.1 Package name.....	12
4.9.2 Package type.....	12
4.9.3 Package overview.....	12
4.9.4 Package objectives.....	12
4.9.5 Package components.....	12
4.10 Evaluation assurance level 7 (EAL7) — Formally verified design and tested.....	13
4.10.1 Package name.....	13
4.10.2 Package type.....	13
4.10.3 Package overview.....	14
4.10.4 Package objectives.....	14
4.10.5 Package components.....	14

5	Composed assurance packages (CAP)	15
5.1	Family name.....	15
5.2	Family overview.....	15
	5.2.1 General.....	15
	5.2.2 Relationship between assurances and assurance packages.....	15
5.3	Family objectives.....	17
5.4	Composed assurance package A (CAP-A) — Structurally composed.....	18
	5.4.1 Package name.....	18
	5.4.2 Package type.....	18
	5.4.3 Package overview.....	18
	5.4.4 Package objectives.....	18
	5.4.5 Package components.....	18
5.5	Composed assurance package B (CAP-B) — Methodically composed.....	19
	5.5.1 Package name.....	19
	5.5.2 Package type.....	19
	5.5.3 Package overview.....	19
	5.5.4 Package objectives.....	19
	5.5.5 Package components.....	20
5.6	Composed assurance package C (CAP-C) — Methodically composed, tested and reviewed.....	20
	5.6.1 Package name.....	20
	5.6.2 Package type.....	20
	5.6.3 Package overview.....	20
	5.6.4 Package objectives.....	20
	5.6.5 Package components.....	21
6	Composite product packages (COMP)	21
6.1	Family name.....	21
6.2	Family overview.....	21
6.3	Family objectives.....	22
6.4	Composite product package 1 (COMP1) — Consistent, integrated, tested and assessed.....	22
	6.4.1 Package name.....	22
	6.4.2 Package type.....	22
	6.4.3 Package overview.....	22
	6.4.4 Package objectives.....	22
	6.4.5 Package components.....	22
7	Protection profile assurances (PPA)	23
7.1	Family name.....	23
7.2	Family overview.....	23
7.3	Family objectives.....	24
7.4	Protection profile assurance DR (PPA-DR) — Direct rationale.....	24
	7.4.1 Package name.....	24
	7.4.2 Package type.....	24
	7.4.3 Package overview.....	24
	7.4.4 Package objectives.....	24
	7.4.5 Package components.....	24
7.5	Protection profile assurance STD (PPA-STD) — Standard.....	24
	7.5.1 Package name.....	24
	7.5.2 Package type.....	24
	7.5.3 Package overview.....	24
	7.5.4 Package objectives.....	25
	7.5.5 Package components.....	25
8	Security target assurances (STA)	25
8.1	Family name.....	25
8.2	Family overview.....	25
8.3	Family objectives.....	26
8.4	Security target assurance DR (STA-DR) — Direct rationale.....	26
	8.4.1 Package name.....	26

8.4.2	Package type.....	26
8.4.3	Package overview.....	26
8.4.4	Package objectives.....	26
8.4.5	Package components.....	26
8.5	Security target assurance STD (STA-STD) — Standard.....	26
8.5.1	Package name.....	26
8.5.2	Package type.....	26
8.5.3	Package overview.....	26
8.5.4	Package objectives.....	27
8.5.5	Package components.....	27

Sample Document

get full document from standards.iteh.ai

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>.

Sample Document

get full document from standards.iteh.ai

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