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 ..... **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

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

concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

NOTE Not all families and components given in ISO/IEC 15408-3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components can be considered for augmentation of an EAL in those Protection Profiles (PPs) and Security Targets (STs) for which they provide utility. Additionally, some classes found in ISO/IEC 15408-3 are not relevant for the EALs. Examples of such classes include class APE (Protection Profile (PP) evaluation) (see ISO/IEC 15408-3:2026,Clause 7) and class ACO (Composition) (see ISO/IEC 15408-3:2026, Clause 15).

A set of assurance components have been chosen for each EAL.

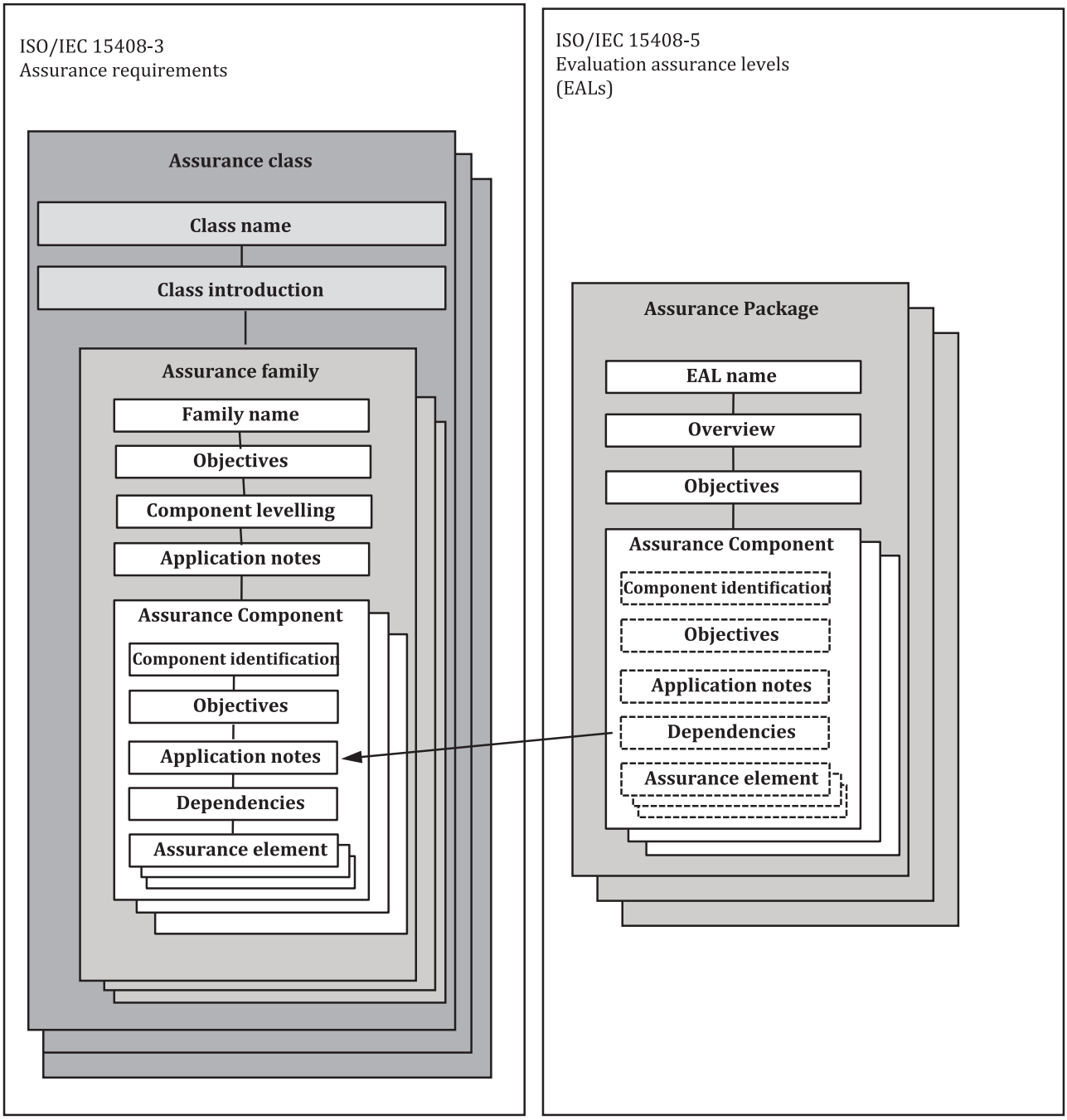
A higher level of assurance than that provided by a given EAL can be achieved by:

— including additional assurance components from other assurance families; or

— replacing an assurance component with a higher-level assurance component from the same assurance family.

4.2.2 Relationship between assurances and assurance levels

Figure 1 illustrates the relationship between the security assurance requirements (SARs) found in ISO/IEC 15408-3 and the assurance levels defined in this document. While assurance components further decompose into assurance elements, assurance elements cannot be individually referenced by assurance levels.



NOTE The arrow in the figure represents a reference from an EAL to an assurance component within the class where it is defined.

Figure 1 — Assurance and assurance level association

Table 1 represents a summary of the EAL.

Table 1 — Evaluation assurance level summary

Assurance class	Assurance Family	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ADV (Development)	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
AGD (Guidance documents)	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
ALC (life cycle support)	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
ASE (Security Target (ST) evaluation)	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
ATE (Tests)	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
AVA (Vulnerability assessment)	AVA_VAN	1	2	2	3	4	5	5

The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

Those items marked in grey are not applicable in the EAL specification. However, they can be used to augment the EAL package.

NOTE Although the ALC_FLR (Flaw remediation) (see ISO/IEC 15408-3:2026, 12.6) and ALC_TDA (TOE development artefacts) (see ISO/IEC 15408-3:2026, 12.8) families are not shown, they are often used as an augmentation to the EALs.

4.3 Family objectives

Seven hierarchically ordered evaluation assurance levels are defined in this document for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from one EAL to another is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope and depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in ISO/IEC 15408-3. More precisely, each EAL includes no more than one component of each assurance family and all the assurance dependencies of every component are addressed.

The notion of "augmentation" allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in ISO/IEC 15408-1, only EALs may be augmented. The notion of an "EAL minus a constituent assurance component" is not recognized in ISO/IEC 15408-1 as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

NOTE An EAL cannot be augmented if it is included in an ST that claims exact conformance to a PP.

4.4 Evaluation assurance level 1 (EAL1) — Functionally tested

4.4.1 Package name

The name of the package is evaluation assurance level 1 (EAL1) — Functionally tested.

4.4.2 Package type

This is an assurance package.

4.4.3 Package overview

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. Where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information, the application of EAL1 is recommended.

EAL1 requires only a limited ST. It is sufficient to simply state the required security functional requirements (SFRs) for the TOE, rather than deriving them from threats, organizational security policies (OSPs) and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation can be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level provides evidence that the TOE functions in a manner consistent with its documentation.

4.4.4 Package objectives

EAL1 **provides a basic level of assurance by a limited ST and an analysis of the SFRs in that ST using a functional and interface specification and guidance documentation, to understand the security behaviour.**

The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functionality (TSF).

EAL1 **also provides assurance through unique identification of the TOE and of the relevant evaluation documents.**

This EAL provides a meaningful increase in assurance over unevaluated IT.

4.4.5 Package components

Table 2 gives the assurance components included in EAL1.

Table 2 — EAL1

Assurance class	Assurance component
ADV (Development)	ADV_FSP.1 (Basic functional specification)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)
ALC (life cycle support)	ALC_CMC.1 (Labelling of the TOE)
	ALC_CMS.1 (TOE CM coverage)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.1 (Security objectives for the operational environment)
	ASE_REQ.1 (Direct rationale security requirements)
	ASE_TSS.1 (TOE summary specification)
ATE (Tests)	ATE_IND.1 (Independent testing - conformance)
AVA (Vulnerability assessment)	AVA_VAN.1 (Vulnerability survey)

4.5 Evaluation assurance level 2 (EAL2) — Structurally tested

4.5.1 Package name

The name of the package is evaluation assurance level 2 (EAL2) — Structurally tested.

4.5.2 Package type

This is an assurance package.

4.5.3 Package overview

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such, it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation can arise when securing legacy systems or where access to the developer can be limited.

4.5.4 Package objectives

EAL2 provides assurance by a **full** ST and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation **and a basic description of the architecture of the TOE,** to understand the security behaviour.

The analysis is supported by:

— **independent testing of** the **TSF;**

— **evidence of developer testing based on the functional specification, selective** independent **confirmation** of the **developer test results; and**

— **a vulnerability analysis (based on the functional specification,** TOE **design,** security **architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a Basic attack potential (see ISO/IEC 15408-1:2026, Clause 3).**

EAL2 also provides assurance through **use** of **a configuration management system** and **evidence** of **secure delivery procedures.**

This EAL **represents** a meaningful increase in assurance **from** EAL1 **by requiring developer testing, a vulnerability analysis (in addition to the search of the public domain) and independent testing based on more detailed TOE specifications.**

4.5.5 Package components

Table 3 gives the assurance components included in EAL2.

Table 3 — EAL2

Assurance class	Assurance component
ADV (Development)	ADV_ARC.1 (Security architecture description)
	ADV_FSP.2 (Security-enforcing functional specification)
	ADV_TDS.1 (Basic design)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)
ALC (life cycle support)	ALC_CMC.2 (Use of the CM system)
	ALC_CMS.2 (Parts of the TOE CM coverage)
	ALC_DEL.1 (Delivery procedures)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.2 (Security objectives)
	ASE_REQ.2 (Derived security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)
ATE (Tests)	ATE_COV.1 (Evidence of coverage)
	ATE_FUN.1 (Functional testing)
	ATE_IND.2 (Independent testing - sample)
AVA (Vulnerability assessment)	AVA_VAN.2 (Vulnerability analysis)

4.6 Evaluation assurance level 3 (EAL3) — Methodically tested and checked

4.6.1 Package name

The name of the package is evaluation assurance level 3 (EAL3) — Methodically tested and checked.

4.6.2 Package type

This is an assurance package.

4.6.3 Package overview

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security and require a thorough investigation of the TOE and its development without substantial re-engineering.

4.6.4 Package objectives

EAL3 provides assurance by a full ST and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and **an architectural** description of the **design** of the TOE, to understand the security behaviour.

The analysis is supported by **independent** testing of the TSF, **evidence** of developer testing based on the functional specification **and TOE design,** selective independent confirmation of the developer test results, and **a** vulnerability analysis (based on the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a Basic attack potential.

EAL3 also provides assurance through **the** use of **development environment controls, TOE** configuration management and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL2 by requiring **more complete** testing **coverage** of the **security functionality** and **mechanisms and/or procedures that provide some confidence that the** TOE **will not be tampered with during development.**

4.6.5 Package components

Table 4 gives the assurance components included in EAL3.

Table 4 — EAL3

Assurance class	Assurance component
ADV (Development)	ADV_ARC.1 (Security architecture description)
	ADV_FSP.3 (Functional specification with complete summary)
	ADV_TDS.2 (Architectural design)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)
ALC (life cycle support)	ALC_CMC.3 (Authorization controls)
	ALC_CMS.3 (Implementation representation CM coverage)
	ALC_DEL.1 (Delivery procedures)
	ALC_DVS.1 (Identification of security controls)
	ALC_LCD.1 (Developer defined life cycle processes)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.2 (Security objectives)
	ASE_REQ.2 (Derived security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)
ATE (Tests)	ATE_COV.2 (Analysis of coverage)
	ATE_DPT.1 (Testing: basic design)
	ATE_FUN.1 (Functional testing)
	ATE_IND.2 (Independent testing - sample)
AVA (Vulnerability assessment)	AVA_VAN.2 (Vulnerability analysis)

4.7 Evaluation assurance level 4 (EAL4) — Methodically designed, tested and reviewed

4.7.1 Package name

The name of the package is evaluation assurance level 4 (EAL4) — Methodically designed, tested and reviewed.

4.7.2 Package type

This is an assurance package.

4.7.3 Package overview

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, although rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.

4.7.4 Package objectives

EAL4 provides assurance by a full ST and an analysis of the SFRs in that ST, using a functional and **complete** interface specification, guidance documentation, **a** description of the **basic modular** design of the TOE **and a subset of the implementation,** to understand the security behaviour.

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results and a vulnerability analysis (based on the functional specification, TOE design, **implementation representation,** security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with **an Enhanced-Basic** attack potential.

EAL4 also provides assurance through the use of development environment controls **and additional** TOE configuration management **including automation** and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL3 by requiring more **design description,** the **implementation representation for the entire TSF** and **improved** mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

4.7.5 Package components

Table 5 gives the assurance components included in EAL4.

Table 5 — EAL4

Assurance class	Assurance component
ADV (Development)	ADV_ARC.1 (Security architecture description)
	ADV_FSP.4 (Complete functional specification)
	ADV_IMP.1 (Implementation representation of the TSF)
	ADV_TDS.3 (Basic modular design)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)

Table 5 *(continued)*

Assurance class	Assurance component
ALC (life cycle support)	ALC_CMC.4 (Production support, acceptance procedures and automation)
	ALC_CMS.4 (Problem tracking CM coverage)
	ALC_DEL.1 (Delivery procedures)
	ALC_DVS.1 (Identification of security controls)
	ALC_LCD.1 (Developer defined life cycle processes)
	ALC_TAT.1 (Well-defined development tools)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.2 (Security objectives)
	ASE_REQ.2 (Derived security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)
ATE (Tests)	ATE_COV.2 (Analysis of coverage)
	ATE_DPT.1 (Testing: basic design)
	ATE_FUN.1 (Functional testing)
	ATE_IND.2 (Independent testing - sample)
AVA (Vulnerability assessment)	AVA_VAN.3 (Focused vulnerability analysis)

4.8 Evaluation assurance level 5 (EAL5) — Semi-formally designed and tested

4.8.1 Package name

The name of the package is evaluation assurance level 5 (EAL5) — Semi-formally designed and tested.

4.8.2 Package type

This is an assurance package.

4.8.3 Package overview

EAL5 permits a developer to gain maximum assurance from security engineering based on rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE is probably designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialized techniques, are not large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.

4.8.4 Package objectives

EAL5 provides assurance by a full ST and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the design of the TOE and the implementation, to understand the security behaviour. **A modular TSF design is also required.**

The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, TOE design, selective independent confirmation of the developer test results and **an independent** vulnerability analysis demonstrating resistance to penetration attackers with **a Moderate** attack potential.

EAL5 also provides assurance through the use of **a** development environment controls, and **comprehensive** TOE configuration management including automation and evidence of secure delivery procedures.

This EAL represents a meaningful increase in assurance from EAL4 by requiring **semi-formal design descriptions, a** more **structured (and hence analysable) architecture** and improved mechanisms and/or procedures that provide confidence that the TOE will not be tampered with during development.

4.8.5 Package components

Table 6 gives the assurance components included in EAL5.

Table 6 — EAL5

Assurance class	Assurance component
ADV (Development)	ADV_ARC.1 (Security architecture description)
	ADV_FSP.5 (Complete semi-formal functional specification with additional error information)
	ADV_IMP.1 (Implementation representation of the TSF)
	ADV_INT.2 (Well-structured internals)
	ADV_TDS.4 (Semi-Formal modular design)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)
ALC (life cycle support)	ALC_CMC.4 (Production support, acceptance procedures and automation)
	ALC_CMS.5 (Development tools CM coverage)
	ALC_DEL.1 (Delivery procedures)
	ALC_DVS.1 (Identification of security controls)
	ALC_LCD.1 (Developer defined life cycle processes)
	ALC_TAT.2 (Compliance with implementation standards)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.2 (Security objectives)
	ASE_REQ.2 (Derived security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)
ATE (Tests)	ATE_COV.2 (Analysis of coverage)
	ATE_DPT.3 (Testing: modular design)
	ATE_FUN.1 (Functional testing)
	ATE_IND.2 (Independent testing - sample)
AVA (Vulnerability assessment)	AVA_VAN.4 (Methodical vulnerability analysis)

4.9 Evaluation assurance level 6 (EAL6) — Semi-formally verified design and tested

4.9.1 Package name

The name of the package is evaluation assurance level 6 (EAL6) — Semi-formally verified design and tested.

4.9.2 Package type

This is an assurance package.

4.9.3 Package overview

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high-risk situations where the value of the protected assets justifies the additional costs.

4.9.4 Package objectives

EAL6 provides assurance by a full ST and an analysis of the SFRs in that ST, using:

— **a** functional and complete interface specification;

— **guidance** documentation; **and**

— **a** description of the design of the TOE and the implementation to understand the security behaviour.

Assurance is **additionally gained through the development** of **a formal representation of** the TSF **(the formal model) and its properties (the formal properties), as defined by** the **SFRs and the security objectives** of the **ST. A modular, layered** and **simple TSF design is also required**.

The analysis is supported by independent testing of the **TSF**, **evidence** of **developer testing based on the functional specification,** TOE **design, selective independent confirmation of the developer test results** and **an independent vulnerability analysis demonstrating resistance to penetration attackers with a High attack potential**.

EAL6 **also provides** assurance **through the use of** a structured **development process, development environment controls,** and **comprehensive TOE configuration management including complete automation, and evidence of secure delivery** procedures.

This EAL represents a meaningful increase in assurance from EAL5 **by requiring more comprehensive analysis, a structured representation of the implementation, more architectural structure (e.g. layering), more comprehensive independent vulnerability analysis and improved configuration management and development environment controls**.

4.9.5 Package components

Table 7 gives the assurance components included in EAL6.

Table 7 — EAL6

Assurance class	Assurance Component
ADV (Development)	ADV_ARC.1 (Security architecture description)
	ADV_FSP.5 (Complete semi-formal functional specification with additional error information)
	ADV_IMP.2 (Complete mapping of the implementation representation of the TSF)
	ADV_INT.3 (Minimally complex internals)
	ADV_SPM.1 (Formal TSF model)
	ADV_TDS.5 (Complete semi-formal modular design)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)
ALC (life cycle support)	ALC_CMC.5 (Advanced support)
	ALC_CMS.5 (Development tools CM coverage)
	ALC_DEL.1 (Delivery procedures)
	ALC_DVS.2 (Sufficiency of security controls)
	ALC_LCD.1 (Developer defined life cycle processes)
	ALC_TAT.3 (Compliance with implementation standards - all parts)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.2 (Security objectives)
	ASE_REQ.2 (Derived security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)
ATE (Tests)	ATE_COV.3 (Rigorous analysis of coverage)
	ATE_DPT.3 (Testing: modular design)
	ATE_FUN.2 (Ordered functional testing)
	ATE_IND.2 (Independent testing - sample)
AVA (Vulnerability assessment)	AVA_VAN.5 (Advanced methodical vulnerability analysis)

4.10 Evaluation assurance level 7 (EAL7) — Formally verified design and tested

4.10.1 Package name

The name of the package is evaluation assurance level 7 (EAL7) — Formally verified design and tested.

4.10.2 Package type

This is an assurance package.

4.10.3 Package overview

EAL7 is applicable to the development of security TOEs for application in extremely high-risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.

4.10.4 Package objectives

EAL7 provides assurance by a full ST and an analysis of the SFRs in that ST, using a functional and complete interface specification, **guidance** documentation, a description of the design of the TOE and **a structured presentation of** the implementation to understand the security behaviour. **Assurance is additionally gained through the development of a formal representation of the TSF (the formal model) and its properties (the formal properties), as defined by the SFRs and the security objectives of the ST. A modular, layered and simple TSF design is also required**.

The analysis is **supported by independent testing** of the TSF, **evidence of developer testing based on** the **functional specification, TOE design** and **implementation representation, complete independent confirmation** of the **developer test results**, and **an independent vulnerability analysis demonstrating resistance to penetration attackers with a High attack potential**.

EAL7 **also provides assurance through the use** of **a structured development process, development environment controls, and comprehensive** TOE **configuration management including complete automation, and evidence** of **secure delivery procedures.**

This EAL represents a meaningful increase in assurance from EAL6 **by requiring more comprehensive analysis using formal representations** and **formal correspondence, and** comprehensive **testing.**

4.10.5 Package components

Table 8 gives the assurance components included in EAL7.

Table 8 — EAL7

Assurance class	Assurance component
ADV (Development)	ADV_ARC.1 (Security architecture description)
	ADV_FSP.6 (Complete semi-formal functional specification with additional formal specification)
	ADV_IMP.2 (Complete mapping of the implementation representation of the TSF)
	ADV_INT.3 (Minimally complex internals)
	ADV_SPM.1 (Formal TSF model)
	ADV_TDS.6 (Complete semi-formal modular design with formal high-level design presentation)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)
ALC (life cycle support)	ALC_CMC.5 (Advanced support)
	ALC_CMS.5 (Development tools CM coverage)
	ALC_DEL.1 (Delivery procedures)
	ALC_DVS.2 (Sufficiency of security controls)
	ALC_LCD.2 (Measurable life cycle model)
	ALC_TAT.3 (Compliance with implementation standards - all parts)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)

Table 8 *(continued)*

Assurance class	Assurance component
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.2 (Security objectives)
	ASE_REQ.2 (Derived security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)
ATE (Tests)	ATE_COV.3 (Rigorous analysis of coverage)
	ATE_DPT.4 (Testing: implementation representation)
	ATE_FUN.2 (Ordered functional testing)
	ATE_IND.3 (Independent testing - complete)
AVA (Vulnerability assessment)	AVA_VAN.5 (Advanced methodical vulnerability analysis)

5 Composed assurance packages (CAP)

5.1 Family name

The name of this family of packages is composed assurance packages (CAPs).

5.2 Family overview

5.2.1 General

The structure of the CAPs is similar to that of the EALs. The main difference between these two types of packages is the type of TOE they apply to. The EALs apply to component TOEs and the CAPs apply to composed TOEs.

A higher level of assurance than that provided by a given CAP can be achieved by:

— including additional assurance components from other assurance families; or

— replacing an assurance component with a higher-level assurance component from the same assurance family.

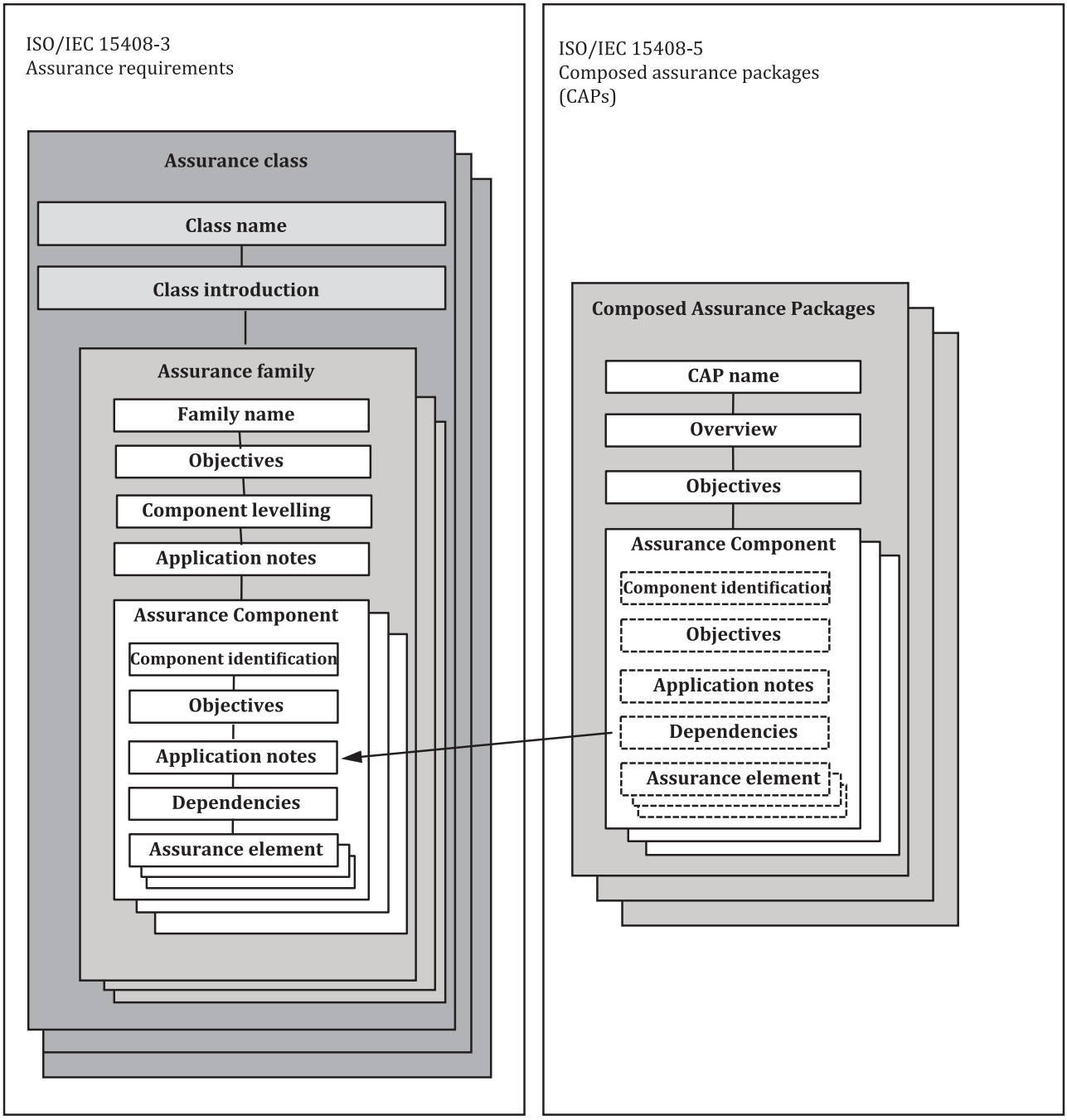
Some dependencies identify the activities performed during the evaluation of the dependent component on which the composed TOE activity relies. Where it is not explicitly identified that the dependency is on a dependent component activity, the dependency is to another evaluation activity of the composed TOE.

The class ACO (Composition) (see ISO/IEC 15408-3:2026**,** Clause 15) components included in the CAP assurance packages shall not be used as augmentations for component TOE evaluations, as this would provide no meaningful assurance for the component.

5.2.2 Relationship between assurances and assurance packages

Figure 2 illustrates the relationship between the SARs and the CAPs defined in this document. While assurance components further decompose into assurance elements, assurance elements cannot be individually referenced by assurance packages.

NOTE While the figure shows the contents of the assurance components, it is intended that this information is included in a CAP by reference to the actual components defined in ISO/IEC 15408-3.



NOTE The arrow in the figure represents a reference from a CAP to an assurance component within the class where it is defined.

Figure 2 — Assurance and composed assurance package (CAP) association

Table 9 represents a summary of the CAP.

Table 9 — Composed assurance package summary

Assurance class	Assurance family	CAP-A	CAP-B	CAP-C
ACO (Composition)	ACO_COR	1	1	1
	ACO_CTT	1	2	2
	ACO_DEV	1	2	3
	ACO_REL	1	1	2
	ACO_VUL	1	2	3
AGD (Guidance documents)	AGD_OPE	1	1	1
	AGD_PRE	1	1	1
ALC (life cycle support)	ALC_CMC	1	1	1
	ALC_CMS	2	2	2
ASE (Security Target (ST) evaluation)	ASE_CCL	1	1	1
	ASE_ECD	1	1	1
	ASE_INT	1	1	1
	ASE_OBJ	1	2	2
	ASE_REQ	1	2	2
	ASE_SPD		1	1
	ASE_TSS	1	1	1

The columns represent a hierarchically ordered set of CAPs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

5.3 Family objectives

The CAPs provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance for composed TOEs.

NOTE There are only a small number of families and components from ISO/IEC 15408-3 included in the CAPs. This is due to their nature of building on evaluation results of previously evaluated entities (base components and dependent components) and does not imply that these do not provide meaningful and desirable assurances.

CAPs shall be applied to composed TOEs, which comprise components that have been, or are going through, component TOE evaluation (see ISO/IEC 15408-3:2026, Annex B). The individual components are certified to an EAL or another assurance package specified in the ST. It is expected that a basic level of assurance in a composed TOE is gained through application of EAL1, which can be achieved with information about the components that is generally available in the public domain. EAL1 can be applied as specified within both component and composed TOEs. CAPs provide an alternative approach to obtaining higher levels of assurance for a composed TOE than application of the EALs above EAL1.

While a dependent component can be evaluated using a previously evaluated and certified base component to satisfy the IT platform requirements in the environment, this does not provide any formal assurance of the interactions between the components or the possible introduction of vulnerabilities resulting from the composition. CAPs consider these interactions and, at higher levels of assurance, ensure that the interface between the components has itself been the subject of testing. A vulnerability analysis of the composed TOE is also performed to consider the possible introduction of vulnerabilities as a result of composing the components.

Three hierarchically ordered CAPs are defined in this document for the rating of a composed TOE's assurance. They are hierarchically ordered inasmuch as each CAP represents more assurance than all lower CAPs. The increase in assurance from CAP to CAP is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements). These increases result in greater analysis of the composition to identify the impact on the evaluation results gained for the individual component TOEs.

These CAPs consist of an appropriate combination of assurance components as described in ISO/IEC 15408-3:2026, Clause 6. More precisely, each CAP includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

The CAPs only consider resistance against an attacker with an attack potential up to Enhanced-Basic. This is due to the level of design information that can be provided through ACO_DEV (Development evidence) (see ISO/IEC 15408-3:2026, 15.3), limiting some of the factors associated with attack potential (knowledge of the composed TOE) and subsequently affecting the rigour of vulnerability analysis that can be performed by the evaluator. Therefore, the level of assurance in the composed TOE is limited, although the assurance in the individual components within the composed TOE may be much higher.

5.4 Composed assurance package A (CAP-A) — Structurally composed

5.4.1 Package name

The name of the package is composed assurance package A (CAP-A) — Structurally composed.

5.4.2 Package type

This is an assurance package.

5.4.3 Package overview

CAP-A is applicable when a composed TOE is integrated and confidence in the correct security operation of the resulting composite is required. This requires the cooperation of the developer of the dependent component in terms of delivery of design information and test results from the dependent component certification, without requiring the involvement of the base component developer.

CAP-A is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record.

5.4.4 Package objectives

CAP-A **provides assurance by analysis of a ST for the composed TOE. The SFRs in the composed TOE ST are analysed using the outputs from the evaluations of the component TOEs (e.g. ST, guidance documentation) and a specification for the interfaces between the component TOEs in the composed TOE to understand the security behaviour.**

The analysis is supported by independent testing of the interfaces of the base component that are relied on by the dependent component, as described in the reliance information, evidence of developer testing based on the reliance information, development information and composition rationale and selective independent confirmation of the developer test results. The analysis is also supported by a vulnerability review of the composed TOE by the evaluator.

CAP-A **also provides assurance through unique identification of the composed TOE (i.e. IT TOE and guidance documentation).**

5.4.5 Package components

Table 10 gives the assurance components included in CAP-A.

Table 10 — CAP-A

Assurance class	Assurance component
ACO (Composition)	ACO_COR.1 (Composition rationale)
	ACO_CTT.1 (Interface testing)
	ACO_DEV.1 (Functional description)
	ACO_REL.1 (Basic reliance information)
	ACO_VUL.1 (Composition vulnerability review)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)
ALC (life cycle support)	ALC_CMC.1 (Labelling of the TOE)
	ALC_CMS.2 (Parts of the TOE CM coverage)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.1 (Security objectives for the operational environment)
	ASE_REQ.1 (Direct rationale security requirements)
	ASE_TSS.1 (TOE summary specification)

5.5 Composed assurance package B (CAP-B) — Methodically composed

5.5.1 Package name

The name of the package is composed assurance package B (CAP-B) — Methodically composed.

5.5.2 Package type

This is an assurance package.

5.5.3 Package overview

CAP-B permits a conscientious developer to gain maximum assurance from understanding, at a subsystem level, the effects of interactions between component TOEs integrated in the composed TOE, while minimizing the demand of involvement of the base component developer.

CAP-B is applicable in those circumstances where developers or users require:

— a moderate level of independently assured security;

— a thorough investigation of the composed TOE and its development without substantial re-engineering.

5.5.4 Package objectives

CAP-B provides assurance by analysis of a **full** ST for the composed TOE. The SFRs in the composed TOE ST are analysed using the outputs from the evaluations of the component TOEs (e.g. ST, guidance documentation), a specification for the interfaces between the component TOEs **and the TOE design (describing TSF subsystems) contained** in the composed **development information** to understand the security behaviour.

The analysis is supported by independent testing of the interfaces of the base component that are relied on by the dependent component, as described in the reliance information **(now also including TOE design),** evidence of developer testing based on the reliance information, development information and composition rationale and selective independent confirmation of the developer test results. The analysis is also supported by a vulnerability **analysis** of the composed TOE by the evaluator **demonstrating resistance to attackers with Basic attack potential.**

This CAP represents a meaningful increase in assurance from CAP-A **by requiring more complete testing coverage** of the **security functionality.**

5.5.5 Package components

Table 11 gives the assurance components included in CAP-B.

Table 11 — CAP-B

Assurance class	Assurance component
ACO (Composition)	ACO_COR.1 (Composition rationale)
	ACO_CTT.2 (Rigorous interface testing)
	ACO_DEV.2 (Basic evidence of design)
	ACO_REL.1 (Basic reliance information)
	ACO_VUL.2 (Composition vulnerability analysis)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)
ALC (life cycle support)	ALC_CMC.1 (Labelling of the TOE)
	ALC_CMS.2 (Parts of the TOE CM coverage)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.2 (Security objectives)
	ASE_REQ.2 (Derived security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)

5.6 Composed assurance package C (CAP-C) — Methodically composed, tested and reviewed

5.6.1 Package name

The name of the package is composed assurance package C (CAP-C) — Methodically composed, tested and reviewed.

5.6.2 Package type

This is an assurance package.

5.6.3 Package overview

CAP-C permits a developer to gain maximum assurance from positive analysis of the interactions between the components of the composed TOE, which, although rigorous, do not require full access to all evaluation evidence of the base component.

CAP-C is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity composed TOEs and are prepared to incur additional security-specific engineering costs.

5.6.4 Package objectives

CAP-C provides assurance by analysis of a full ST for the composed TOE. The SFRs in the composed TOE ST are analysed using the outputs from the evaluations of the component TOEs (e.g. ST, guidance documentation), a specification for the interfaces between the component TOEs and the TOE design (describing TSF **modules)** contained in the composed development information to understand the security behaviour.

The analysis is supported by independent testing of the interfaces of the base component that are relied on by the dependent component, as described in the reliance information (now including TOE design), evidence of developer testing based on the reliance information, development information and composition rationale, and selective independent confirmation of the developer test results. The analysis is also supported by a vulnerability analysis of the composed TOE by the evaluator demonstrating resistance to attackers with **Enhanced-Basic** attack potential.

This CAP represents a meaningful increase in assurance from CAP-B by requiring more **design description and demonstration** of **resistance to a higher attack potential.**

5.6.5 Package components

Table 12 gives the assurance components included in CAP-C.

Table 12 — CAP-C

Assurance class	Assurance component
ACO (Composition)	ACO_COR.1 (Composition rationale)
	ACO_CTT.2 (Rigorous interface testing)
	ACO_DEV.3 (Detailed evidence of design)
	ACO_REL.2 (Reliance information)
	ACO_VUL.3 (Enhanced-Basic composition vulnerability analysis)
AGD (Guidance documents)	AGD_OPE.1 (Operational user guidance)
	AGD_PRE.1 (Preparative procedures)
ALC (life cycle support)	ALC_CMC.1 (Labelling of the TOE)
	ALC_CMS.2 (Parts of the TOE CM coverage)
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.2 (Security objectives)
	ASE_REQ.2 (Derived security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)

6 Composite product packages (COMP)

6.1 Family name

The name of this family of packages is composite product packages (COMPs).

6.2 Family overview

COMP provides assurance that a composite product has been assembled and evaluated according to the relevant criteria.

Table 13 represents a summary of the COMP.

Table 13 — Composite product package summary

Assurance class	Assurance Family	COMP1
ADV (Development)	ADV_COMP	1
ALC (life cycle support)	ALC_COMP	1
ASE (Security Target (ST) evaluation)	ASE_COMP	1
ATE (Tests)	ATE_COMP	1
AVA (Vulnerability assessment)	AVA_COMP	1

Each number in the resulting matrix identifies a specific assurance component where applicable.

6.3 Family objectives

Assurance components of COMP are applicable when composite evaluation techniques according to ISO/IEC 15408-1:2026, 14.3.3 are used for a composite product. The objectives are to ensure that:

— the TOE has been composed of an already evaluated base component and a dependent component, considering the requirements given in ISO/IEC 15408-1 and ISO/IEC 15408-3;

— the evaluation of STs, life cycle requirements, design, testing and vulnerability analysis for the composite product have been performed according to the criteria specified in ISO/IEC 15408-3.

These objectives provide assurance that potential contradictions, inconsistencies or security gaps resulting from the composition of the base component and the dependent component of the composite product have been considered and are not present.

6.4 Composite product package 1 (COMP1) — Consistent, integrated, tested and assessed

6.4.1 Package name

The name of the package is composite product package 1 (COMP1) — Consistent, integrated, tested and assessed.

6.4.2 Package type

This is an assurance package.

6.4.3 Package overview

COMP1 is applicable when a composite product combined of an already evaluated base component and a dependent component is evaluated. The composite evaluation approach supports the reuse of the evaluation results previously achieved for the base component.

6.4.4 Package objectives

COMP1 **provides assurance by analysis of the composite product that potential contradictions, inconsistencies or security gaps resulting from the composition of its (already evaluated) base component and dependent component do not exist. This analysis covers the STs, life cycle requirements, design, testing and vulnerability analysis for the composite product by using the criteria specified in ISO/IEC 15408-3**.

6.4.5 Package components

Table 14 gives the assurance components included in COMP1.

Table 14 — COMP1

Assurance class	Assurance component
ADV (Development)	ADV_COMP.1 (Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority)
ALC (life cycle support)	ALC_COMP.1 (Integration of the dependent component into the related base component and Consistency check for delivery and acceptance procedures)
ASE (Security Target (ST) evaluation)	ASE_COMP.1 (Consistency of Security Target (ST))
ATE (Tests)	ATE_COMP.1 (Composite product functional testing)
AVA (Vulnerability assessment)	AVA_COMP.1 (Composite product vulnerability assessment)

7 Protection profile assurances (PPA)

7.1 Family name

The name of this family of packages is protection profile assurances (PPAs).

7.2 Family overview

The PPA family provides two assurance packages for PP evaluation:

— assurance package for evaluating direct rationale PPs;

— assurance package for evaluating standard PPs.

These assurance packages provide the components that are used in the evaluation of each type of PP described in ISO/IEC 15408-1.

PPAs consist of an appropriate combination of assurance components as described in class APE (Protection Profile (PP) evaluation) (see ISO/IEC 15408-3:2026, Clause 7). More precisely, each PPA includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

Table 15 represents a summary of the PPA.

Table 15 — Protection profile assurance summary

Assurance class	Assurance family	PPA-DR	PPA-STD
APE (Protection Profile (PP) evaluation)	APE_CCL	1	1
	APE_ECD	1	1
	APE_INT	1	1
	APE_OBJ	1	2
	APE_REQ	1	2
	APE_SPD	1	1

The columns represent the set of PPAs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

7.3 Family objectives

The PPA objectives are to support the provision of assurance through evaluation that a protection profile conforms with the requirements given in ISO/IEC 15408-1.

7.4 Protection profile assurance DR (PPA-DR) — Direct rationale

7.4.1 Package name

The name of the package is protection profile assurance DR (PPA-DR) — Direct rationale.

7.4.2 Package type

This is an assurance package.

7.4.3 Package overview

PPA-DR provides assurance by evaluation of a direct rationale protection profile, using the criteria specified in ISO/IEC 15408-3.

7.4.4 Package objectives

PPA-DR **is applicable when a direct rationale PP is evaluated. It can be used to verify that a direct rationale PP conforms with the requirements of ISO/IEC 15408-1**.

7.4.5 Package components

Table 16 gives the assurance components included in PPA-DR.

Table 16 — PPA-DR

Assurance class	Assurance component
APE (Protection Profile (PP) evaluation)	APE_CCL.1 (Conformance claims)
	APE_ECD.1 (Extended components definition)
	APE_INT.1 (PP introduction)
	APE_OBJ.1 (Security objectives for the operational environment)
	APE_REQ.1 (Direct rationale security requirements)
	APE_SPD.1 (Security problem definition)

7.5 Protection profile assurance STD (PPA-STD) — Standard

7.5.1 Package name

The name of the package is protection profile assurance STD (PPA-STD) — Standard.

7.5.2 Package type

This is an assurance package.

7.5.3 Package overview

PPA-STD provides assurance by evaluation of a standard PP, using the criteria specified in ISO/IEC 15408-3.

7.5.4 Package objectives

PPA-STD is applicable when a **standard** PP is evaluated. It can be used to verify that a **standard** PP conforms with the requirements of ISO/IEC 15408-1.

7.5.5 Package components

Table 17 gives the assurance components included in PPA-STD.

Table 17 — PPA-STD

Assurance class	Assurance component
APE (Protection Profile (PP) evaluation)	APE_CCL.1 (Conformance claims)
	APE_ECD.1 (Extended components definition)
	APE_INT.1 (PP introduction)
	APE_OBJ.2 (Security objectives)
	APE_REQ.2 (Derived security requirements)
	APE_SPD.1 (Security problem definition)

8 Security target assurances (STA)

8.1 Family name

The name of this family of packages is security target assurances (STAs).

8.2 Family overview

The STA family provides two assurance packages for ST evaluation:

— assurance package for evaluating direct rationale STs;

— assurance package for evaluating standard STs.

These assurance packages provide the components that are used in the evaluation of each type of security target described in ISO/IEC 15408-1.

STAs consist of an appropriate combination of assurance components as described in class ASE (Security Target (ST) evaluation) (see ISO/IEC 15408-3:2026, Clause 9). More precisely, each STA includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

Table 18 represents a summary of the STA.

Table 18 — Security target assurance summary

Assurance class	Assurance Family	STA-DR	STA-STD
ASE (Security Target (ST) evaluation)	ASE_CCL	1	1
	ASE_ECD	1	1
	ASE_INT	1	1
	ASE_OBJ	1	2
	ASE_REQ	1	2
	ASE_SPD	1	1
	ASE_TSS	1	1

The columns represent the set of STAs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

8.3 Family objectives

The STA objectives are intended to support the provision of assurance through evaluation, to ensure that a security target conforms with the requirements given in ISO/IEC 15408-1.

8.4 Security target assurance DR (STA-DR) — Direct rationale

8.4.1 Package name

The name of the package is security target assurance DR (STA-DR) — Direct rationale.

8.4.2 Package type

This is an assurance package.

8.4.3 Package overview

STA-DR provides assurance by evaluation of a direct rationale ST, using the criteria specified in ISO/IEC 15408-3.

8.4.4 Package objectives

STA-DR **is applicable when a direct rationale ST is evaluated. It can be used to verify that a direct rationale ST conforms with the requirements of ISO/IEC 15408-1**.

8.4.5 Package components

Table 19 gives the assurance components included in STA-DR.

Table 19 — STA-DR

Assurance class	Assurance component
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.1 (Security objectives for the operational environment)
	ASE_REQ.1 (Direct rationale security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)

8.5 Security target assurance STD (STA-STD) — Standard

8.5.1 Package name

The name of the package is security target assurance STD (STA-STD) — Standard.

8.5.2 Package type

This is an assurance package.

8.5.3 Package overview

STA-STD provides assurance by evaluation of a standard ST, using the criteria specified in ISO/IEC 15408-3.

8.5.4 Package objectives

STA-STD is applicable when a **standard** ST is evaluated. It **may** be used to verify that a **standard** ST conforms with the requirements of ISO/IEC 15408-1.

8.5.5 Package components

Table 20 gives the assurance components included in STA-STD.

Table 20 — STA-STD

Assurance class	Assurance component
ASE (Security Target (ST) evaluation)	ASE_CCL.1 (Conformance claims)
	ASE_ECD.1 (Extended components definition)
	ASE_INT.1 (ST introduction)
	ASE_OBJ.2 (Security objectives)
	ASE_REQ.2 (Derived security requirements)
	ASE_SPD.1 (Security problem definition)
	ASE_TSS.1 (TOE summary specification)

ICS 35.030
Price based on 27 pages