DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 15408-5

ISO/IEC JTC **1**/SC **27**	Secretariat: **DIN**
Voting begins on: **2020-05-29**	Voting terminates on: **2020-08-21**

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

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

ICS: 35.030

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

This document is circulated as received from the committee secretariat.

Reference number
ISO/IEC DIS 15408-5:2020(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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.

This document was prepared by Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

A list of all parts in the ISO/IEC 15408 series can be found on the ISO website.

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.

This is the first edition of ISO/IEC 15408-5.

Introduction

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

ISO/IEC 15408-1 defines the term "package" and describes the fundamental concepts.

This document presents:

- *evaluation assurance level (EAL)* 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 TOE.
- *composition assurance (CAP)* 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 (COMP)* package 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 Assurance (PPA)* 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 Assurance (STA)* family of packages that specify sets of security assurance components used for specifying appropriate security assurances to be provided during a Security Target evaluation.

The audience for this document includes consumers, developers, and evaluators of secure IT products.

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 have been identified as useful in support of common usage by stakeholders.

EXAMPLE Examples of provided packages include the evaluation assurance levels (EAL) and the composed assurance packages (CAPs).

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, *Information security, cybersecurity and privacy protection— Evaluation criteria for IT security — Part 1: Introduction and general requirements*

ISO/IEC 15408-3, *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 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

- IEC Electropedia: available at http://www.electropedia.org/
- ISO Online browsing platform: available at http://www.iso.org/obp

4 Evaluation Assurance Levels

4.1 Family Name

The name of this family of packages is *Evaluation Assurance Levels (EALs)*.

4.2 Evaluation assurance level (EAL) overview

4.2.1 General

The Evaluation Assurance Levels (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 will 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 the APE and ACO classes.

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:

a) including additional assurance components from other assurance families; or

b) 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 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.

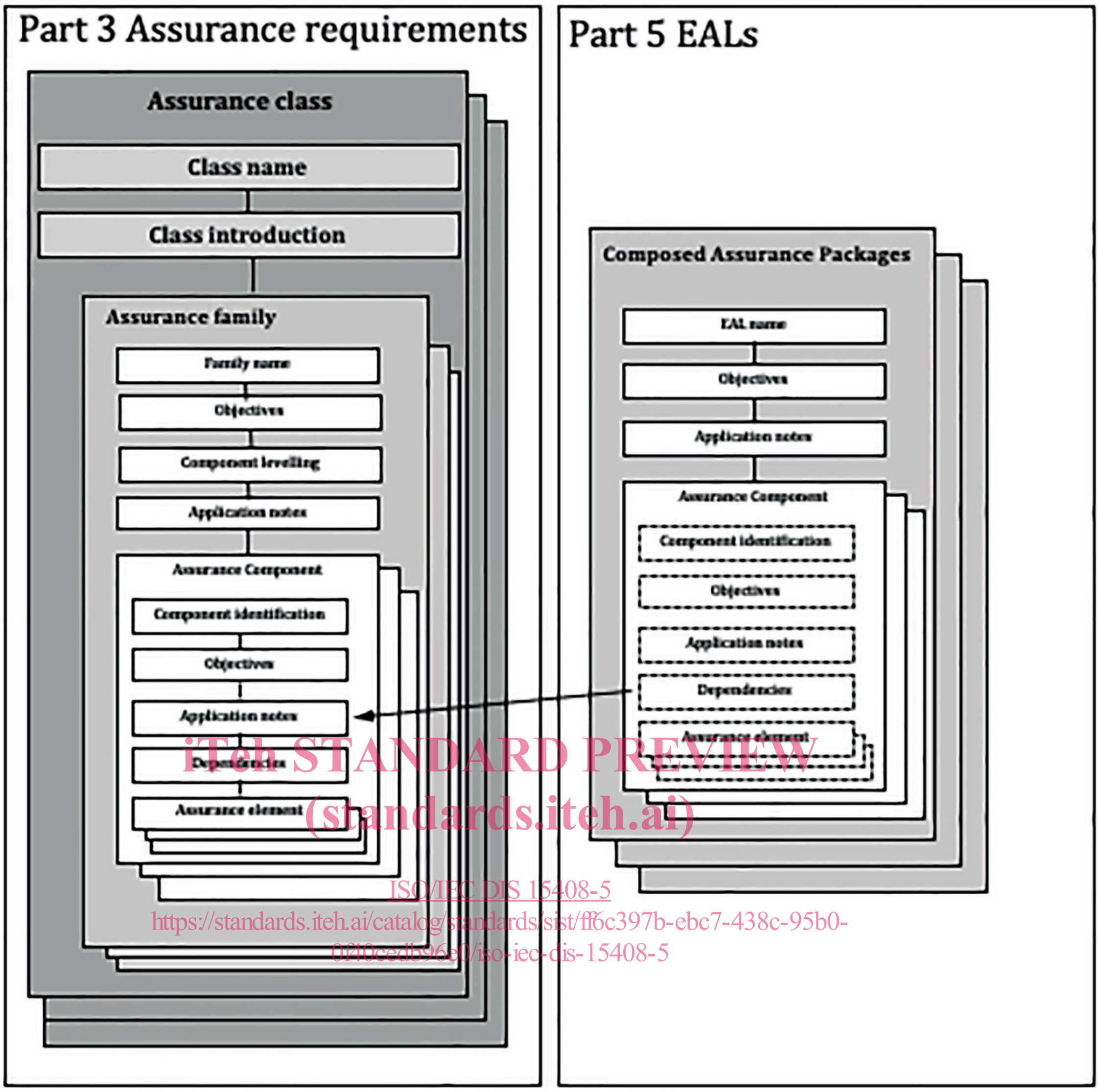

Figure 1 — Assurance and assurance level association

Table 1 represents a summary of the EALs. 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 may be used to augment the EAL package.

NOTE Although the ALC_FLR and ALC_TDA families are not shown in Table 1, they are often used as an augmentation to the EALs.

Table 1 — Evaluation assurance level summary

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
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**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
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
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
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**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

4.3 Evaluation assurance level (EAL) objectives

As outlined in 4.4, 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 EAL to EAL 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 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 by the standard 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 levels

4.4.1 General

Subclause 4.4 provides definitions of the EALs, highlighting differences between the specific requirements and the prose characterisations of those requirements using bold type.

4.4.2 Evaluation assurance level 1 (EAL1) - functionally tested

4.4.2.1 Package Name

The name of the package is: *Evaluation assurance level 1 (EAL1) - functionally tested.*

4.4.2.2 Package Type

This is an assurance Package.

4.4.2.3 Package overview

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value 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.

EAL1 requires only a limited ST. It is sufficient to simply state the required SFRs for the TOE, rather than deriving them from threats, 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 could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

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

4.4.2.4 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 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.

4.4.2.5 Assurance components

Table 2 gives the assurance components included in EAL 1.

Table 2 — EAL1

Assurance Class	Assurance components
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: 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 Stated security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.1 Independent testing - conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

4.4.3 Evaluation assurance level 2 (EAL2) - structurally tested

4.4.3.1 Package Name

The name of the package is: *Evaluation assurance level 2 (EAL2) –structurally tested.*

4.4.3.2 Package Type

This is an assurance Package.

4.4.3.3 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 may arise when securing legacy systems, or where access to the developer may be limited.

4.4.3.4 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 upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.**

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