



BSI Standards Publication

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

Part 5: Pre-defined packages of security requirements

National foreword

This British Standard is the UK implementation of EN ISO/IEC 15408-5:2023. It is identical to ISO/IEC 15408-5:2022. It supersedes BS ISO/IEC 15408-5:2022, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33, Information security, cybersecurity and privacy protection.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2023
Published by BSI Standards Limited 2023

ISBN 978 0 539 28232 0

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 August 2022.

Amendments/corrigenda issued since publication

Date	Text affected
31 December 2023	This corrigendum renumbers BS ISO/IEC 15408-5:2022 as BS EN ISO/IEC 15408-5:2023

English version

Information security, cybersecurity and privacy protection
- Evaluation criteria for IT security - Part 5: Pre-defined
packages of security requirements (ISO/IEC 15408-
5:2022)

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 (ISO/IEC 15408-
5:2022)

Informationssicherheit, Cybersicherheit und Schutz
der Privatsphäre - Evaluationskriterien für IT-
Sicherheit - Teil 5: Vordefinierte Pakete von
Sicherheitsanforderungen (ISO/IEC 15408-5:2022)

This European Standard was approved by CEN on 20 November 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.



CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

European foreword

The text of ISO/IEC 15408-5:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 15408-5:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by June 2024, and conflicting national standards shall be withdrawn at the latest by June 2024.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 15408-5:2022 has been approved by CEN-CENELEC as EN ISO/IEC 15408-5:2023 without any modification.

Contents

Page

Foreword	v
Introduction	vii
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 Evaluation assurance levels	2
4.1 Family name	2
4.2 Evaluation assurance level overview	2
4.2.1 General	2
4.2.2 Relationship between assurances and assurance levels	2
4.3 Evaluation assurance level objectives	4
4.4 Evaluation assurance levels	5
4.4.1 General	5
4.4.2 Evaluation assurance level 1 (EAL1) — Functionally tested	5
4.4.3 Evaluation assurance level 2 (EAL2) — Structurally tested	6
4.4.4 Evaluation assurance level 3 (EAL3) — Methodically tested and checked	7
4.4.5 Evaluation assurance level 4 (EAL4) — Methodically designed, tested and reviewed	9
4.4.6 Evaluation assurance level 5 (EAL5) — Semi-formally verified designed and tested	10
4.4.7 Evaluation assurance level 6 (EAL6) — Semi-formally verified design and tested	11
4.4.8 Evaluation assurance level 7 (EAL7) — Formally verified design and tested	13
5 Composed assurance packages (CAPs)	14
5.1 Family name	14
5.2 Composed assurance package (CAP) overview	15
5.2.1 General	15
5.2.2 Relationship between assurances and assurance packages	15
5.3 Composed assurance package (CAP) objectives	16
5.4 Packages in the CAP family	18
5.4.1 Composition assurance package A — Structurally composed	18
5.4.2 Composition assurance package B — Methodically composed	19
5.4.3 Composition assurance package C — Methodically composed, tested and reviewed	20
6 Composite product package	21
6.1 Package name	21
6.2 Package type	21
6.3 Package overview	21
6.4 Objectives	22
6.5 Security assurance components	22
7 Protection profile assurances	22
7.1 Family name	22
7.2 PPA family overview	22
7.3 PPA family objectives	23
7.4 PPA packages	23
7.4.1 Protection profile assurance package — Direct rationale PP	23
7.4.2 Protection profile assurance package — Standard	24
8 Security target assurances	24
8.1 Family name	24
8.2 STA family overview	25
8.3 STA family objectives	25

8.4	STA packages.....	25
8.4.1	Security target assurance package — Direct rationale.....	25
8.4.2	Security target assurance package — Standard.....	26

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).

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) or the IEC list of patent declarations received (see <https://patents.iec.ch>).

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*.

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 and www.iec.ch/national-committees.

Legal notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations (called CC), they hereby grant non-exclusive license to ISO/IEC to use CC in the continued development/maintenance of the ISO/IEC 15408 series of standards. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC as they see fit.

Australia	The Australian Signals Directorate
Canada	Communications Security Establishment
France	Agence Nationale de la Sécurité des Systèmes d'Information
Germany	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Netherlands	Netherlands National Communications Security Agency
New Zealand	Government Communications Security Bureau
Republic of Korea	National Security Research Institute
Spain	Ministerio de Asuntos Económicos y Transformación Digital
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency

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.

NOTE This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

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).

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 target of evaluation (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 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 15408-1:2022, *Information security, cybersecurity and privacy protection— Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-3:2022, *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, definitions and abbreviated terms 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

4.1 Family name

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

4.2 Evaluation assurance level 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 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 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.