

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

## EESTI STANDARDI EESSÕNA

## NATIONAL FOREWORD

<p>See Eesti standard EVS-EN ISO/IEC 15408-5:2023 sisaldab Euroopa standardi EN ISO/IEC 15408-5:2023 ingliskeelset teksti.</p> <p>Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.</p> <p>Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 06.12.2023.</p> <p>Standard on kättesaadav Eesti Standardimis- ja Akrediteerimiskeskusest.</p>	<p>This Estonian standard EVS-EN ISO/IEC 15408-5:2023 consists of the English text of the European standard EN ISO/IEC 15408-5:2023.</p> <p>This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.</p> <p>Date of Availability of the European standard is 06.12.2023.</p> <p>The standard is available from the Estonian Centre for Standardisation and Accreditation.</p>
--	---

Tagasisidet standardi sisu kohta on võimalik edastada, kasutades EVS-i veebilehel asuvat tagasiside vormi või saates e-kirja meiliaadressile [standardiosakond@evs.ee](mailto:standardiosakond@evs.ee).

ICS 35.030

Standardite reprodutseerimise ja levitamise õigus kuulub Eesti Standardimis- ja Akrediteerimiskeskusele. Andmete paljundamine, taastekitamine, kopeerimine, salvestamine elektroonsesse süsteemi või edastamine ükskõik millises vormis või millisel teel ilma Eesti Standardimis- ja Akrediteerimiskeskuse kirjaliku loata on keelatud.

Kui Teil on küsimusi standardite autorikaitse kohta, võtke palun ühendust Eesti Standardimis- ja Akrediteerimiskeskusega: Koduleht [www.evs.ee](http://www.evs.ee); telefon 605 5050; e-post [info@evs.ee](mailto:info@evs.ee)

The right to reproduce and distribute standards belongs to the Estonian Centre for Standardisation and Accreditation. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying, without a written permission from the Estonian Centre for Standardisation and Accreditation.

If you have any questions about copyright, please contact Estonian Centre for Standardisation and Accreditation: Homepage [www.evs.ee](http://www.evs.ee); phone +372 605 5050; e-mail [info@evs.ee](mailto:info@evs.ee)

ICS 35.030

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
<b>Foreword</b> .....	<b>v</b>
<b>Introduction</b> .....	<b>vii</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>2</b>
<b>4 Evaluation assurance levels</b> .....	<b>2</b>
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
<b>5 Composed assurance packages (CAPs)</b> .....	<b>14</b>
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
<b>6 Composite product package</b> .....	<b>21</b>
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
<b>7 Protection profile assurances</b> .....	<b>22</b>
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
<b>8 Security target assurances</b> .....	<b>24</b>
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

This document is a preview generated by EVS

## 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://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.

**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*