SLOVENSKI STANDARD
oSIST prEN ISO/IEC 15408-5:2023

01-oktober-2023

Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Merila za vrednotenje varnosti IT - 5. del: Vnaprej določeni paketi varnostnih zahtev (ISO/IEC 15408-5:2022)

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

Informationstechnik - IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit - Teil 5: Vordefinierte Pakete von Sicherheitsanforderungen (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)

Ta slovenski standard je istoveten z: prEN ISO/IEC 15408-5

ICS:

35.030   Informacijska varnost   IT Security

oSIST prEN ISO/IEC 15408-5:2023   en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

INTERNATIONAL STANDARD

ISO/IEC 15408-5

First edition
2022-08

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

ISO/IEC 15408-5:2022(E)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

COPYRIGHT PROTECTED DOCUMENT

Contents

Page

ISO/IEC 15408-5:2022(E)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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.

iTeh STANDARD PREVIEW

(standards.iteh.ai)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

Part 5: Pre-defined packages of security requirements

1 Scope

This document provides packages of security assurance and security functional requirements that 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.