SLOVENSKI STANDARD
oSIST prEN ISO/IEC 15408-1:2024

01-november-2024

Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Merila za vrednotenje varnosti IT - 1. del: Uvod in splošni model (ISO/IEC DIS 15408-1:2024)

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 1: Introduction and general model (ISO/IEC DIS 15408-1:2024)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit - Teil 1: Einführung und allgemeines Modell

Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Partie 1: Introduction et modèle général (ISO/IEC DIS 15408-1:2024)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 15408-1**

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 15408-1:2024 **en,fr,de**

DRAFT International Standard

ISO/IEC DIS 15408-1

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

Part 1: Introduction and general model

Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information —

Partie 1: Introduction et modèle général

ICS: 35.030

ISO/IEC JTC **1**/SC **27**

Secretariat: **DIN**

Voting begins on:
2024-08-19

Voting terminates on:
2024-11-11

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

Reference number
ISO/IEC DIS 15408-1:2024(en)

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

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 Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fifth edition cancels and replaces the fourth edition (ISO/IEC 15408-1:2022), which has been technically revised.

The changes are as follows:

— the terminology has been reviewed and updated: the definitions of *multi-assurance security target* and *multi-assurance PP-Configuration* have been added, the definition of *multi-assurance evaluation* has been improved for accuracy, and the term *sub-TOE security functionality* has been removed;

— the package conformance claim for security targets, protection profiles and PP-Modules, respectively, has been reviewed and aligned with ISO/IEC 18045;

— the specification of multiple PP-Modules Bases has been improved for accuracy;

— several errors, mistakes and typos have been corrected, including references to clauses of the standard.

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.

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	Centro Criptológico Nacional
Sweden	FMV, Swedish Defence Materiel Administration
United Kingdom	National Cyber Security Centre
United States	The National Security Agency and the National Institute of Standards and Technology

Introduction

The ISO/IEC 15408 series permits comparability between the results of independent security evaluations by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware, or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

The ISO/IEC 15408 series is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

The ISO/IEC 15408 series is intentionally flexible, enabling a range of evaluation approaches to be applied to a range of security properties of a range of IT products. Therefore, users of the standard are cautioned to exercise care that this flexibility is not misused. For example, using the ISO/IEC 15408 series in conjunction with unsuitable evaluation methods/activities, irrelevant security properties, or inappropriate IT products, can result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties, and methods to determine that an evaluation provides meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

The ISO/IEC 15408 series addresses the protection of assets from unauthorized disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively. The ISO/IEC 15408 series may also be applicable to aspects of IT security outside of these three categories. The ISO/IEC 15408 series is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. The ISO/IEC 15408 series may be applied in other areas of IT but makes no claim of applicability in these areas.

Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of the ISO/IEC 15408 series. Some of these are identified below:

a) the ISO/IEC 15408 series does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognized that significant security can often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls;

b) the ISO/IEC 15408 series does not address the evaluation methodology under which the criteria should be applied;

NOTE 1 The baseline methodology is defined in ISO/IEC 18045. ISO/IEC 15408-4 can be used to further derive evaluation activities and methods from ISO/IEC 18045.

c) the ISO/IEC 15408 series does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that the ISO/IEC 15408 series is intended to be used for evaluation purposes in the context of such a framework;

d) the procedures for use of evaluation results in accreditation are outside the scope of the ISO/IEC 15408 series. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors must make separate provisions for those aspects;

e) the subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in the ISO/IEC 15408 series. In the case that independent assessment of mathematical

properties of cryptography is required, the evaluation scheme under which the ISO/IEC 15408 series is applied shall make provision for such assessments.

The following notes appears in other parts of the ISO/IEC 15408 series and in ISO/IEC 18045 to describe the use of bold and italic type in those documents. This document does not use those conventions, but the notes have been retained for alignment with the rest of the series.

NOTE 1 This document uses bold type to highlight hierarchical relationships between requirements. This convention calls for the use of bold type for all new requirements.

NOTE 2 For security functional requirements, the use of italics denotes assignment and selection items.

NOTE 3 For security assurance requirements, special verbs relating to mandatory evaluation activities are presented in bold italic type face.

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

Part 1: Introduction and general model

1 Scope

This document establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the standard which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

This document provides an overview of all parts of the ISO/IEC 15408 series. It describes the various parts of the ISO/IEC 15408 series; defines the terms and abbreviations to be used in all parts of the standard; establishes the core concept of a Target of Evaluation (TOE); describes the evaluation context and describes the audience to which the evaluation criteria is addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

This document introduces:

— the key concepts of protection profiles (PP), PP-Modules, PP-Configurations, packages, security targets (ST), and conformance types;

— a description of the organization of security components throughout the model;

— the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 can be tailored through the use of permitted operations;

— general information about the evaluation methods given in ISO/IEC 18045;

— guidance for the application of ISO/IEC 15408-4 in order to develop evaluation methods (EM) and evaluation activities (EA) derived from ISO/IEC 18045;

— general information about the pre-defined Evaluation Assurance Levels (EALs) defined in ISO/IEC 15408-5;

— information in regard to the scope of evaluation schemes.

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 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *IT security techniques — Methodology for IT security evaluation*

ISO/IEC IEEE 24765, *Systems and software engineering — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 18045 and ISO/IEC IEEE 24765 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/

3.1
action
documented activity of the *evaluator* (3.45) or *developer* (3.33)

Note 1 to entry: Evaluator actions and developer actions are required by ISO/IEC 15408-3.

3.2
administrator
entity (3.36) that has a level of trust with respect to all policies implemented by the *TOE security functionality (TSF)* (3.95)

Note 1 to entry: Not all *protection profiles (PPs)* (3.70) or *security targets (STs)* (3.84) assume the same level of trust for administrators. Typically, administrators are assumed to adhere at all times to the policies in the ST of the *target of evaluation (TOE)* (3.92). Some of these policies can be related to the functionality of the TOE, while others can be related to the *operational environment* (3.65).

3.3
adverse action
action (3.1) performed by a *threat agent* (3.93) on an *asset* (3.4)

3.4
asset
entity (3.36) that the owner of the *target of evaluation (TOE)* (3.92) presumably places value on

3.5
assignment
specification of an identified parameter in a functional or assurance component

3.6
assurance
grounds for confidence that a *target of evaluation (TOE)* (3.92) meets the *security functional requirements (SFRs)* (3.80)

3.7
assurance package
named set of *security assurance requirements* (3.78)

EXAMPLE “EAL3”.

3.8
attack potential
measure of the effort needed to exploit a vulnerability in a *target of evaluation (TOE)* (3.92)

Note 1 to entry: The effort is expressed as a function of properties related to the attacker (e.g. expertise, resources, and motivation) and properties related to the vulnerability itself (e.g. window of opportunity, time to exposure).

3.9
attack surface
set of logical or physical interfaces to a target, consisting of points through which access to the target and its functions may be attempted

EXAMPLE 1 The casing of a payment terminal is a part of physical attack surface for that device.