Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities (ISO/IEC 15408-4:2022)

EESTI STANDARDIMIS- JA AKREDITEERIMISKESKUS
ESTONIAN CENTRE FOR STANDARDISATION AND ACCREDITATION

EESTI STANDARDI EESSÕNA

NATIONAL FOREWORD

See Eesti standard EVS-EN ISO/IEC 15408-4:2023 sisaldab Euroopa standardi EN ISO/IEC 15408-4:2023 ingliskeelset teksti.	This Estonian standard EVS-EN ISO/IEC 15408-4:2023 consists of the English text of the European standard EN ISO/IEC 15408-4:2023.
Standard on jõustunud sellekohase teate avaldamisega EVS Teatajas.	This standard has been endorsed with a notification published in the official bulletin of the Estonian Centre for Standardisation and Accreditation.
Euroopa standardimisorganisatsioonid on teinud Euroopa standardi rahvuslikele liikmetele kättesaadavaks 06.12.2023.	Date of Availability of the European standard is 06.12.2023.
Standard on kättesaadav Eesti Standardimis-ja Akrediteerimiskeskusest.	The standard is available from the Estonian Centre for Standardisation and Accreditation.

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

ICS 35.030

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 15408-4

December 2023

ICS 35.030

English version

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities (ISO/IEC 15408-4:2022)

Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Partie 4: Cadre prévu pour la spécification des méthodes d'évaluation et des activités connexes (ISO/IEC 15408-4:2022)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit - Teil 4: Rahmen für die Festlegung von Bewertungsmethoden und -tätigkeiten (ISO/IEC 15408-4:2022)

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 15408-4:2022 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 15408-4:2023 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 15408-4:2022 has been approved by CEN-CENELEC as EN ISO/IEC 15408-4:2023 without any modification.

Contents

Page

Foreword ... **iv**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 General model of evaluation methods and evaluation activities ... **1**
4.1 Concepts and model ... 1
4.2 Deriving evaluation methods and evaluation activities ... 3
4.3 Verb usage in the description of evaluation methods and evaluation activities ... 5
4.4 Conventions for the description of evaluation methods and evaluation activities ... 6
5 Structure of an evaluation method ... **6**
5.1 Overview ... 6
5.2 Specification of an evaluation method ... 7
5.2.1 Overview ... 7
5.2.2 Identification of evaluation methods ... 8
5.2.3 Entity responsible for the evaluation method ... 9
5.2.4 Scope of the evaluation method ... 9
5.2.5 Dependencies ... 9
5.2.6 Required input from the developer or other entities ... 9
5.2.7 Required tool types ... 10
5.2.8 Required evaluator competences ... 10
5.2.9 Requirements for reporting ... 10
5.2.10 Rationale for the evaluation method ... 10
5.2.11 Additional verb definitions ... 12
5.2.12 Set of evaluation activities ... 12
6 Structure of evaluation activities ... **12**
6.1 Overview ... 12
6.2 Specification of an evaluation activity ... 12
6.2.1 Unique identification of the evaluation activity ... 12
6.2.2 Objective of the evaluation activity ... 12
6.2.3 Evaluation activity links to SFRs, SARs, and other evaluation activities ... 13
6.2.4 Required input from the developer or other entities ... 13
6.2.5 Required tool types ... 13
6.2.6 Required evaluator competences ... 13
6.2.7 Assessment strategy ... 13
6.2.8 Pass/fail criteria ... 14
6.2.9 Requirements for reporting ... 15
6.2.10 Rationale for the evaluation activity ... 15
Bibliography ... **16**

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.

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. ISO/IEC 18045 provides a companion methodology for some of the assurance requirements specified in the ISO/IEC 15408 series.

The model of security evaluation in ISO/IEC 15408-1 identifies that high-level generic evaluation activities are defined in ISO/IEC 18045, but that more specific evaluation activities (EAs) can be defined as technology-specific adaptations of these generic activities for particular evaluation contexts, e.g. for security functional requirements (SFRs)or security assurance requirements (SARs) applied to specific technologies or target of evaluation (TOE) types. Specification of such evaluation activities is already occurring amongst practitioners and this creates a need for a specification for defining such evaluation activities.

This document describes a framework that can be used for deriving evaluation activities from work units of ISO/IEC 18045 and grouping them into evaluation methods (EMs). Evaluation activities or evaluation methods can be included in protection profiles (PPs) and any documents supporting them. Where a PP, PP-Configuration, PP-Module, package, or Security Target (ST) identifies that specific evaluation methods/evaluation activities are to be used, then the evaluators are required by ISO/IEC 18045 to follow and report the relevant evaluation methods/evaluation activities when assigning evaluator verdicts. As noted in ISO/IEC 15408-1, in some cases an evaluation authority can decide not to approve the use of particular evaluation methods/evaluation activities: in such a case, the evaluation authority can decide not to carry out evaluations following an ST that requires those evaluation methods/evaluation activities.

This document also allows for evaluation activities to be defined for extended SARs, in which case derivation of the evaluation activities relates to equivalent action elements and work units defined for that extended SAR. Where reference is made in this document to the use of ISO/IEC 18045 or ISO/IEC 15408-3 for SARs (such as when defining rationales for evaluation activities), then, in the case of an extended SAR, the reference applies instead to the equivalent action elements and work units defined for that extended SAR.

For clarity, this document specifies how to define evaluation methods and evaluation activities but does not itself specify instances of evaluation methods or evaluation activities.

The following NOTE 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 NOTE has been retained for alignment with the rest of the series.

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 4: Framework for the specification of evaluation methods and activities

1 Scope

This document provides a standardized framework for specifying objective, repeatable and reproducible evaluation methods and evaluation activities.

This document does not specify how to evaluate, adopt, or maintain evaluation methods and evaluation activities. These aspects are a matter for those originating the evaluation methods and evaluation activities in their particular area of interest.

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 model*

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

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

ISO/IEC 18045, *Information security, cybersecurity and privacy protection — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, the terms and definitions in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, and ISO/IEC 18045 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 General model of evaluation methods and evaluation activities

4.1 Concepts and model

ISO/IEC 18045 defines a generic set of work units that an evaluator carries out in order to reach a verdict for most of the assurance classes, families and components defined in ISO/IEC 15408-3. The