SLOVENSKI STANDARD
oSIST prEN ISO/IEC 15408-4:2024

01-november-2024

Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Merila za vrednotenje varnosti IT - 4. del: Okvir za specifikacijo metod vrednotenja in dejavnosti (ISO/IEC DIS 15408-4:2024)

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 4: Framework for the specification of evaluation methods and activities (ISO/IEC DIS 15408-4:2024)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit - Teil 4: Rahmen für die Festlegung von Bewertungsmethoden und -tätigkeiten

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 DIS 15408-4:2024)

Ta slovenski standard je istoveten z: **prEN ISO/IEC 15408-4**

ICS:

35.030	Informacijska varnost	IT Security

oSIST prEN ISO/IEC 15408-4:2024 **en,fr,de**

DRAFT
International
Standard

ISO/IEC
DIS
15408-4

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

Part 4: Framework for the specification of evaluation methods and activities

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

ICS: ISO ics

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 15408-4:2024(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) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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).

ISO draws attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO takes no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents. ISO shall not be held responsible for identifying any or all such patent rights.

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.

This document was prepared by Joint 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 15408-2:2022), which has been technically revised.

The main changes are as follows:

— Minor typographical errors corrected.

A list of all parts in the ISO 15408 series can be found on the ISO website.

The catalogue of security assurance requirements defined in this document is provided in machine readable format (XML) at: https://standards.iso.org/iso-iec/TBD.

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.

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. 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 evaluator 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 evaluator 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 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 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, definitions and abbreviated terms

For the purposes of this document, the terms, definitions, and abbreviated terms given in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 15408-5, ISO/IEC 18045 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at www.iso.org/obp;

— IEC Electropedia: available at 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 relationship between the structure of a SAR in ISO/IEC 15408-3 and the work units in ISO/IEC 18045 is described in ISO/IEC 18045 and summarized in Figure 1.

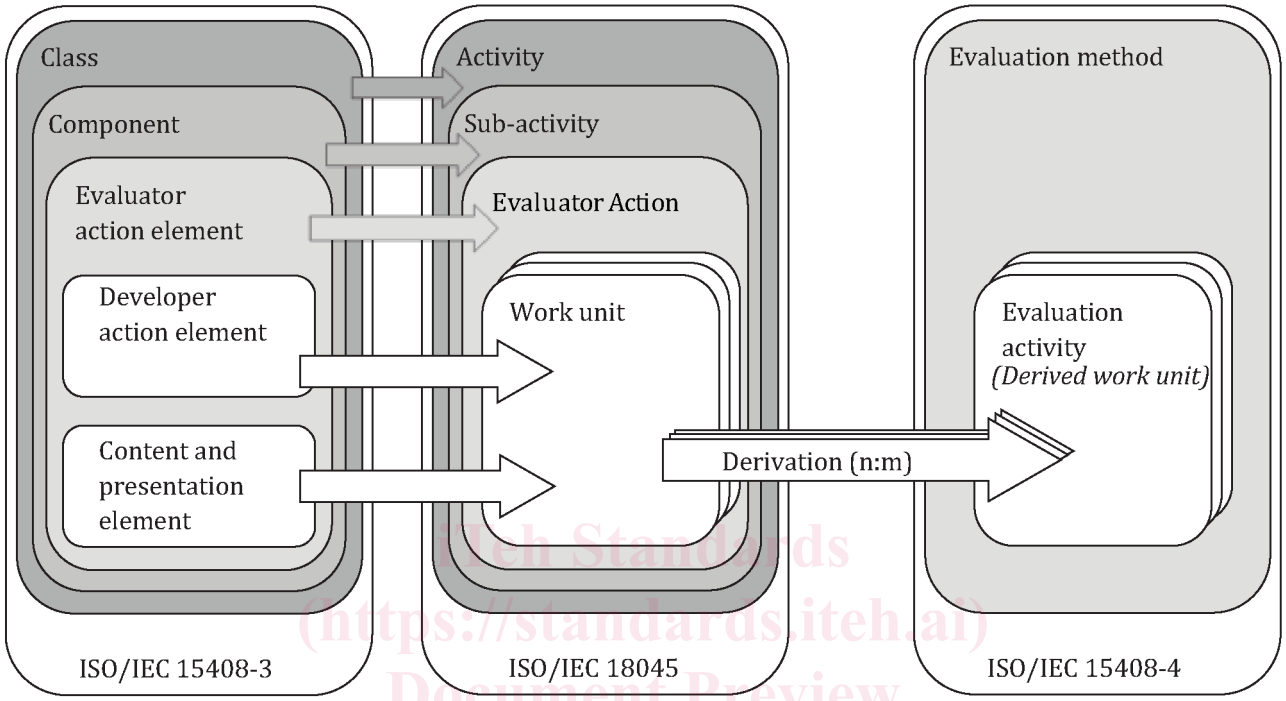

Figure 1 — Mapping of ISO/IEC 15408-3 and ISO/IEC 18045 to structures of this document

For the purposes of defining new evaluation methods and evaluation activities, the main point to note is that each action (representing an evaluator action element in ISO/IEC 15408-3 or an implied evaluator action element) is represented in ISO/IEC 18045 as a set of work units that are carried out by an evaluator.

This document specifies the ways in which new evaluation activities can be derived from the generic work units in ISO/IEC 18045, and combined into an evaluation method that is intended for use in some particular evaluation context. A typical example of such an evaluation context would be a particular TOE type or particular technology type.

EXAMPLE 1

— TOE type: a network device

— Technology type: specific cryptographic functions

If evaluation methods and evaluation activities are required to be used with a particular PP, PP-Module or PP-Configuration, then a PP or PP-Module or PP-Configuration shall identify this requirement in its conformance statement. If evaluation methods and evaluation activities are required to be used with a particular package, then the package shall identify this requirement in the security requirement section. If Evaluation Methods and Evaluation Activities are claimed by an ST as a result of that ST claiming conformance to a PP, PP-Configuration, or package, then the ST shall identify the EMs/EAs used in its conformance claim. No formal claim of conformance to ISO/IEC 15408-4 is made in any of these cases (the contents of PPs, PP-Modules, PP-Configurations and packages are described in more detail in ISO/IEC 15408-1).