# SLOVENSKI STANDARD
# oSIST prEN ISO/IEC 15408-4:2023

**01-oktober-2023**

---

**Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Merila za vrednotenje varnosti IT - 4. del: Okvir za specifikacijo metod vrednotenja in dejavnosti (ISO/IEC 15408-4:2022)**

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)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Informationstechnik - IT-Sicherheitsverfahren - Evaluationskriterien für IT-Sicherheit - Teil 4: Rahmen für die Festlegung von Bewertungsmethoden und -tätigkeiten (ISO/IEC 15408-4:2022)

oSIST prEN ISO/IEC 15408-4:2023
https://standards.iteh.ai/catalog/standards/sist/194d817d-a71e-4110-b496-4c2c9ef74ee7/osist-pren-iso-iec-15408-4-2023

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)

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

---

**ICS:**

| | | |
|---|---|---|
| 35.030 | Informacijska varnost | IT Security |

**oSIST prEN ISO/IEC 15408-4:2023** **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

oSIST prEN ISO/IEC 15408-4:2023

iTeh STANDARD PREVIEW
(standards.iteh.ai)

oSIST prEN ISO/IEC 15408-4:2023
https://standards.iteh.ai/catalog/standards/sist/194d817d-a71e-4110-b496-4c2c9ef74ee7/osist-pren-iso-iec-15408-4-2023

oSIST prEN ISO/IEC 15408-4:2023

INTERNATIONAL STANDARD

# ISO/IEC 15408-4

First edition
2022-08

# 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*

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN ISO/IEC 15408-4:2023
https://standards.iteh.ai/catalog/standards/sist/f94d0f7d-a71e-4110-b496-4c2c9ef74ee7/osist-pren-iso-iec-15408-4-2023

Reference number
ISO/IEC 15408-4:2022(E)

© ISO/IEC 2022

oSIST prEN ISO/IEC 15408-4:2023



iTeh STANDARD PREVIEW
(standards.iteh.ai)

oSIST prEN ISO/IEC 15408-4:2023
https://standards.iteh.ai/catalog/standards/sist/194d817d-a71e-4110-b496-4c2c9ef74ee7/osist-pren-iso-iec-15408-4-2023

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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



© ISO/IEC 2022 – All rights reserved

oSIST prEN ISO/IEC 15408-4:2023



# 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**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN ISO/IEC 15408-4:2023
https://standards.iteh.ai/catalog/standards/sist/194d817d-a71e-4110-b496-4c2c9ef74ee7/osist-pren-iso-iec-15408-4-2023

© ISO/IEC 2022 – All rights reserved

oSIST prEN ISO/IEC 15408-4:2023



# 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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.

oSIST prEN ISO/IEC 15408-4:2023
https://standards.iteh.ai/catalog/standards/sist/904d8a7d-a7ce-4100-b496-4c2c9ef74ee7/osist-pren-iso-iec-15408-4-2023

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.


© ISO/IEC 2022 – All rights reserved

oSIST prEN ISO/IEC 15408-4:2023



# 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 |

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN ISO/IEC 15408-4:2023
https://standards.iteh.ai/catalog/standards/sist/194d817d-a71e-4110-b496-4c2c9ef74ee7/osist-pren-iso-iec-15408-4-2023

© ISO/IEC 2022 – All rights reserved

oSIST prEN ISO/IEC 15408-4:2023



# 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/7d2a1fc9-1f10-4e9d-9ed5-ec7c0ab
prEN-ISO-IEC-15408-4-2023

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.

 © ISO/IEC 2022 – All rights reserved

oSIST prEN ISO/IEC 15408-4:2023



# 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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
oSIST prEN ISO/IEC 15408-4:2023
https://standards.iteh.ai/catalog/standards/sist/194d817d-a71e-4110-b496-4c2c9ef74ee7/osist-pren-iso-iec-15408-4-2023

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

© ISO/IEC 2022 – All rights reserved 

oSIST prEN ISO/IEC 15408-4:2023



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.

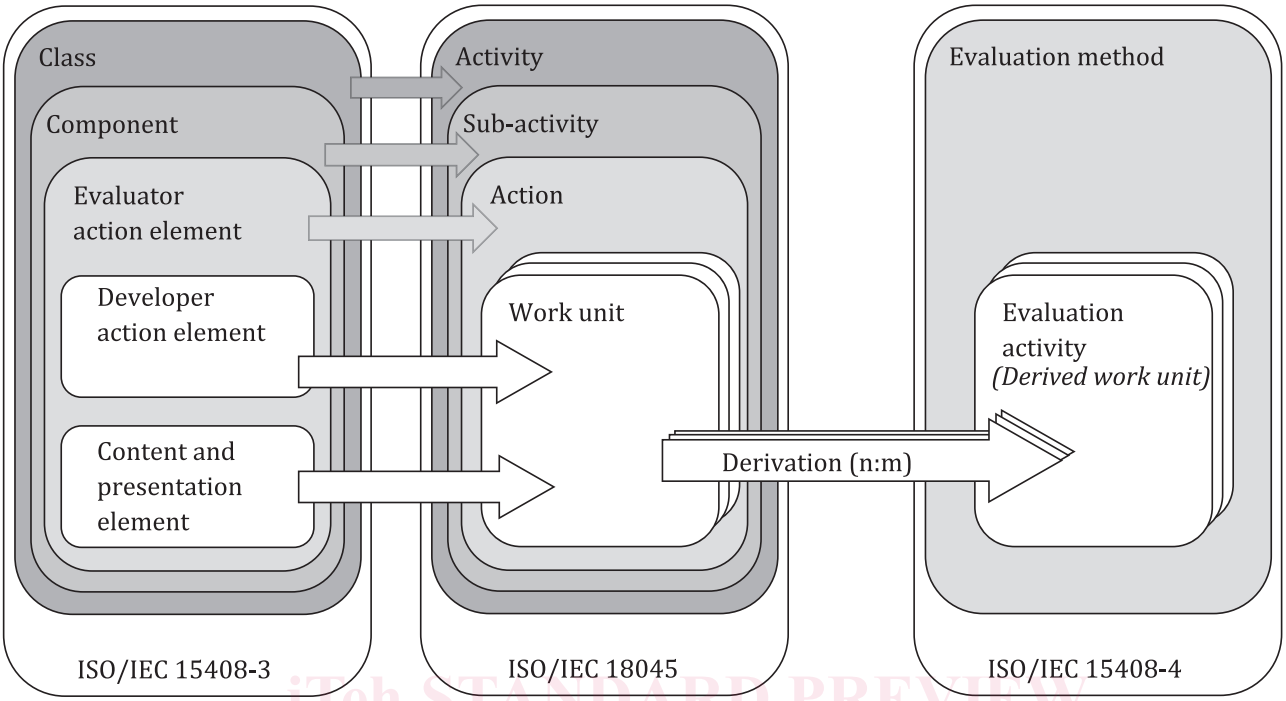


**Figure 1 — Mapping of ISO/IEC 15408-3 and ISO/IEC 18045 structures to structures of this document**

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 15408-4:2022
https://standards.iteh.ai/catalog/standards/sist/0f0e2e7d-4f1f-4f7d-b22e-2f1f4e7f7b5a/iso-iec-15408-4-2022
prEN ISO/IEC 15408-4:2023

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, 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).

A PP, PP-Configuration, PP-Module or package may use more than one evaluation method or separate set of evaluation activities.

EXAMPLE 2 Multiple evaluation methods can be used where separate evaluation methods have been defined for cryptographic operations and for secure channel protocols used in a PP.


© ISO/IEC 2022 – All rights reserved

oSIST prEN ISO/IEC 15408-4:2023



NOTE Where exact conformance is used, ISO/IEC 15408-1 states that evaluation methods/evaluation activities are not allowed to be defined in a PP-Configuration: the evaluation methods/evaluation activities to be used are included in the PPs and PP-Modules and not in the PP-Configuration).

When a PP, PP-Module, PP-Configuration, or package identifies that certain evaluation methods/evaluation activities are to be used, then this is done using a standard wording that states the requirement and references the definition of the evaluation methods/evaluation activities to be used. An ST shall only identify required evaluation methods and evaluation activities that are included in a PP, PP-Module, PP-Configuration or package to which the ST claims conformance (i.e. the ST itself shall not add, modify or remove any evaluation methods or evaluation activities). An ST shall include identification of all evaluation methods/evaluation activities that it requires (i.e. including any that are required by PPs, PP-Modules, PP-Configurations, or packages to which the ST claims conformance), so that there is a single list that can be checked and referenced by evaluators and readers of the ST.

Evaluation methods and evaluation activities may be defined within the document that requires them (e.g. as part of a PP), or externally in a different document (or in a combination of both). Although identification is required as described above, it is not necessary to reproduce the text of the evaluation methods/evaluation activities in other documents (e.g, an ST does not have to include the full text of the evaluation methods/evaluation activities from a PP to which it claims conformance).

## 4.2 Deriving evaluation methods and evaluation activities

In general, defining evaluation activities and evaluation methods may start either from an SAR, aiming to make some or all parts of its work units more specific, or from an SFR, aiming to define specific aspects of work units related to that SFR.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

When starting from an SAR, a guideline for the process is as follows.

a) Identify the relevant ISO/IEC 18045 work units from which to derive at least one individual evaluation activity or groups of evaluation activities.

oSIST prEN ISO/IEC 15408-4:2023
https://standards.iteh.ai/catalog/standards/sist/194d817d-a71e-4110-b496-4c2c9ef74ee7/osist-

b) For each work unit from which an evaluation activity is derived:

   1) define the new evaluation activities in terms of the specific work to be carried out and evaluation criteria as described in 6.2 (including, if required, pass/fail criteria as described in 6.2.8);

   2) group evaluation activities into an evaluation method if necessary;

   3) state the rationale for the new evaluation activities and the evaluation method under which they are grouped as described in 5.2.10 and 6.2.10.

      EXAMPLE A rationale can include reference to the developer action, and content and presentation elements of the work units from which they are derived.

A guideline for starting from an SFR would be as follows.

a) Identify the relevant SFR.

b) Identify the SARs (from ISO/IEC 15408-3 or a set of extended SARs, or both) to be addressed for that particular SFR, and the corresponding ISO/IEC 18045 work units.

c) Define the new evaluation activities in terms of the specific work to be carried out and evaluation criteria as described in 6.2 (including, if required, pass/fail criteria as described in 6.2.8).

   EXAMPLE Evaluation activities can be defined to examine the presentation of a specific SFR in the TOE Summary Specification (derived from ASE), to examine the presentation of the SFR in the guidance documentation (derived from AGD), and to carry out specific tests of the SFR (derived from ATE).

d) Map the affected work units for the SARs to the new evaluation activities.

© ISO/IEC 2022 – All rights reserved 