# SLOVENSKI STANDARD
# oSIST prEN ISO/IEC 18045:2024

**01-oktober-2024**

---

**Informacijska varnost, kibernetska varnost in varovanje zasebnosti - Merila za ocenjevanje varnosti IT - Metodologija za ocenjevanje varnosti IT (ISO/IEC DIS 18045:2024)**

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation (ISO/IEC DIS 18045:2024)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit - Methodik für die Bewertung der IT-Sicherheit (ISO/IEC DIS 18045:2024)

Sécurité de l'information, cybersécurité et protection de la vie privée - Critères d'évaluation pour la sécurité des technologies de l'information - Méthodologie pour l'évaluation de sécurité (ISO/IEC DIS 18045:2024)



**Ta slovenski standard je istoveten z:** **prEN ISO/IEC 18045**

---

**ICS:**

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

**oSIST prEN ISO/IEC 18045:2024** **en,fr,de**

# DRAFT International Standard

# ISO/IEC DIS 18045

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

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

ICS: 35.030



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

Secretariat: **DIN**

Voting begins on:
**2024-08-14**

Voting terminates on:
**2024-11-06**

This document is circulated as received from the committee secretariat.

**ISO/CEN PARALLEL PROCESSING**



Reference number
ISO/IEC DIS 18045:2024(en)

## COPYRIGHT PROTECTED DOCUMENT



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/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 second/third/... edition cancels and replaces the first/second/... edition (ISO #####:####), which has been technically revised.

The main changes are as follows:



— xxx xxxxxxx xxx xxxx

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

The catalogue of security evaluation 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 Methodology for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Methodology for Information Technology Security Evaluations (called CEM), they hereby grant non-exclusive license to ISO/IEC to use CEM in the continued development/maintenance of the ISO/IEC 18045 International Standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CEM 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<br>National Institute of Standards and Technology |

# Introduction

The target audience for this document is primarily evaluators applying the ISO/IEC 15408 series and certifiers confirming evaluator actions. Evaluation sponsors, developers, protection profile (PP), PP-Module, PP-Configuration, and security target (ST) authors, and other parties interested in IT security, can be a secondary audience.

This document cannot answer all questions concerning IT security evaluation and further interpretations may be needed. Individual schemes determine how to handle such interpretations, although these can be subject to mutual recognition agreements. A list of methodology-related activities that can be handled by individual schemes can be found in Annex A.

This document is intended to be used in conjunction with the ISO/IEC 15408 series. Reference throughout the document to ISO/IEC 15408 implies the ISO/IEC 15408 series.

NOTE 1 This document uses bold italic type face to identify special verbs relating to mandatory evaluation activities.

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

## 1 Scope

This document defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 series evaluation, using the criteria and evaluation evidence defined in the ISO/IEC 15408 series.

## 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 15408-4, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

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

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

## 3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms, definitions, and abbreviated terms given in the ISO/IEC 15408 series, ISO/IEC IEEE 24765 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.

**3.1**
**check (verb)**
⟨evaluation⟩ generate a verdict by a simple comparison

Note 1 to entry: Evaluator expertise is not required. The statement that uses this verb describes what is mapped.

**3.2**
**confirm (verb)**
⟨evaluation⟩ declare that something has been reviewed in detail with an independent determination of sufficiency

Note 1 to entry: The level of rigour required depends on the nature of the subject matter.

**3.3**
**demonstrate (verb)**
⟨evaluation⟩ provide a conclusion gained by an analysis which is less rigorous than a "proof"

**3.4**
**describe (verb)**
⟨evaluation⟩ provide specific details of an entity

**3.5**
**determine (verb)**
⟨evaluation⟩ affirm a particular conclusion based on independent analysis with the objective of reaching a particular conclusion

Note 1 to entry: The usage of this term implies a truly independent analysis, usually in the absence of any previous analysis having been performed. Compare with the terms *confirm* (3.2) or *verify* (3.23) which imply that an analysis has already been performed which needs to be reviewed.

**3.6**
**elapsed time**
total amount of time taken by an attacker to identify that a particular potential vulnerability may exist in the TOE, to develop an attack method and to sustain effort required to mount the attack against the TOE



**3.7**
**ensure (verb)**
⟨evaluation⟩ guarantee a strong causal relationship between an action and its consequences

Note 1 to entry: When "ensure" is preceded by the word "help" it indicates that the consequence is not fully certain, on the basis of that action alone.



**3.8**
**evaluation evidence**
item used as a basis for establishing the verdict of an evaluation activity

**3.9**
**examine (verb)**
⟨evaluation⟩ generate a verdict by analysis using evaluator expertise

Note 1 to entry: The statement that uses this verb identifies what is analysed and the properties for which it is analysed.

**3.10**
**exhaustive (adj)**
⟨evaluation⟩ characteristic of a methodical approach taken to perform an analysis or activity according to an unambiguous plan

Note 1 to entry: This term is used in respective parts of the ISO/IEC 15408 series with respect to conducting an analysis or other activity. It is related to "systematic" but is considerably stronger, in that it indicates not only that a methodical approach has been taken to perform the analysis or activity according to an unambiguous plan, but that the plan that was followed is sufficient to *ensure* (3.7) that all possible avenues have been exercised.

**3.11**
**explain (verb)**
⟨evaluation⟩ give argument accounting for the reason for taking a course of action

Note 1 to entry: This term differs from both *describe* (3.4) and *demonstrate* (3.3). It is intended to answer the question "Why?" without actually attempting to argue that the course of action that was taken was necessarily optimal.