International Standard

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

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 de spécification de méthodes et activités d'évaluation

Second edition
2026-05

Reference number
ISO/IEC 15408-4:2026(en)

© ISO/IEC 2026



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2026

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

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms, definitions and abbreviated terms **1**
4 General model of evaluation methods and evaluation activities **2**
4.1 Concepts and model 2
4.2 Deriving evaluation methods and evaluation activities 3
4.3 Verb usage in the description of evaluation methods and evaluation activities 6
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 8
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**

© ISO/IEC 2026 – All rights reserved

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).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take 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 and IEC 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 and https://patents.iec.ch. ISO and IEC 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. 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*, in collaboration with the European Committee for Standardization (CEN) Technical Committee CEN/CLC/JTC 13, *Cybersecurity and data protection*, in accordance with the Agreement on technical cooperation between ISO and CEN (Vienna Agreement).

This second edition cancels and replaces the first edition (ISO/IEC 15408-4:2022), which has been technically revised.

The main changes are as follows:

— minor typographical and editorial errors corrected.

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 2026 – All rights reserved

Introduction

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 must be used, 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.

Several governmental organizations have 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. More information on these agencies can be found at https://commoncriteriaportal.org/cc/copyright/index.cfm.

© ISO/IEC 2026 – All rights reserved

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 specifies requirements and 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 15408-3:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045:2026, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Requirements and methodology for IT security evaluation*

3 Terms, definitions and abbreviated terms

For the purposes of this document, the terms and definitions given in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, 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/

© ISO/IEC 2026 – All rights reserved