

---

---

**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*





**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](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

Page

<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>vi</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Normative references</b> .....	<b>1</b>
<b>3 Terms and definitions</b> .....	<b>1</b>
<b>4 General model of evaluation methods and evaluation activities</b> .....	<b>1</b>
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
<b>5 Structure of an evaluation method</b> .....	<b>6</b>
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
<b>6 Structure of evaluation activities</b> .....	<b>12</b>
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
<b>Bibliography</b> .....	<b>16</b>

## 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](http://www.iso.org/directives) or [www.iec.ch/members\\_experts/refdocs](http://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](http://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](http://www.iso.org/iso/foreword.html). In the IEC, see [www.iec.ch/understanding-standards](http://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](http://www.iso.org/members.html) and [www.iec.ch/national-committees](http://www.iec.ch/national-committees).

## 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