



SLOVENSKI STANDARD
oSIST prEN ISO/IEC 18045:2024

01-oktober-2024

Informacijska varnost, kibernetika 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)

<https://standards.iteh.ai>

<https://standards.iteh.ai/catalog/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-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

[oSIST prEN ISO/IEC 18045:2024](https://standards.iteh.ai/catalog/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-18045-2024)

<https://standards.iteh.ai/catalog/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-18045-2024>

This document is circulated as received from the committee secretariat.

ISO/CEN PARALLEL PROCESSING

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

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-08-14

Voting terminates on:
2024-11-06

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENTS AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

© ISO/IEC 2024

ISO/IEC DIS 18045:2024(en)

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[oSIST prEN ISO/IEC 18045:2024](https://standards.iteh.ai/catalog/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-18045-2024)

<https://standards.iteh.ai/catalog/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-18045-2024>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

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 DIS 18045:2024(en)

Contents

	Page
Foreword	vii
Introduction	ix
1 Scope	1
2 Normative references	1
3 Terms, definitions and abbreviated terms	1
4 Terminology	4
5 Verb usage	4
6 General evaluation guidance	4
7 Relationship between the ISO/IEC 15408 series and ISO/IEC 18045 structures	4
8 Evaluation process and related tasks	5
8.1 General.....	5
8.2 Evaluation process overview.....	6
8.2.1 Objectives.....	6
8.2.2 Responsibilities of the roles.....	6
8.2.3 Relationship of roles.....	6
8.2.4 General evaluation model.....	6
8.2.5 Evaluator verdicts.....	7
8.3 Evaluation input task.....	9
8.3.1 Objectives.....	9
8.3.2 Application notes.....	9
8.3.3 Management of evaluation evidence sub-task.....	10
8.4 Evaluation sub-activities.....	10
8.5 Evaluation output task.....	10
8.5.1 Objectives.....	10
8.5.2 Management of evaluation outputs.....	11
8.5.3 Application notes.....	11
8.5.4 Write OR sub-task.....	11
8.5.5 Write ETR sub-task.....	11
9 Class APE Protection Profile (PP) evaluation	18
9.1 Introduction.....	18
9.1.1 Re-using the evaluation results of certified PPs.....	18
9.2 Conformance claims (APE_CCL).....	19
9.2.1 Evaluation of sub-activity (APE_CCL.1).....	19
9.3 Extended components definition (APE_ECD).....	29
9.3.1 Evaluation of sub-activity (APE_ECD.1).....	29
9.4 PP introduction (APE_INT).....	33
9.4.1 Evaluation of sub-activity (APE_INT.1).....	33
9.5 Security objectives (APE_OBJ).....	34
9.5.1 Evaluation of sub-activity (APE_OBJ.1).....	34
9.5.2 Evaluation of sub-activity (APE_OBJ.2).....	36
9.6 Security requirements (APE_REQ).....	38
9.6.1 Evaluation of sub-activity (APE_REQ.1).....	38
9.6.2 Evaluation of sub-activity (APE_REQ.2).....	44
9.7 Security problem definition (APE_SPD).....	48
9.7.1 Evaluation of sub-activity (APE_SPD.1).....	48
10 Class ACE Protection Profile Configuration evaluation	50
10.1 Introduction.....	50
10.2 PP-Module conformance claims (ACE_CCL).....	51
10.2.1 Evaluation of sub-activity (ACE_CCL.1).....	51
10.3 PP-Configuration consistency (ACE_CCO).....	57
10.3.1 Evaluation of sub-activity (ACE_CCO.1).....	57

ISO/IEC DIS 18045:2024(en)

10.4	PP-Module extended components definition (ACE_ECD)	65
10.4.1	Evaluation of sub-activity (ACE_ECD.1)	65
10.5	PP-Module introduction (ACE_INT)	69
10.5.1	Evaluation of sub-activity (ACE_INT.1)	69
10.6	PP-Module consistency (ACE_MCO)	72
10.6.1	Evaluation of sub-activity (ACE_MCO.1)	72
10.7	PP-Module security objectives (ACE_OBJ)	75
10.7.1	Evaluation of sub-activity (ACE_OBJ.1)	75
10.7.2	Evaluation of sub-activity (ACE_OBJ.2)	77
10.8	PP-Module security requirements (ACE_REQ)	80
10.8.1	Evaluation of sub-activity (ACE_REQ.1)	80
10.8.2	Evaluation of sub-activity (ACE_REQ.2)	85
10.9	PP-Module security problem definition (ACE_SPD)	90
10.9.1	Evaluation of sub-activity (ACE_SPD.1)	90
11	Class ASE Security Target (ST) evaluation	92
11.1	Introduction	92
11.2	Application notes	92
11.2.1	Re-using the evaluation results of certified PPs	92
11.2.2	Composition	92
11.3	Conformance claims (ASE_CCL)	93
11.3.1	Evaluation of sub-activity (ASE_CCL.1)	93
11.4	Consistency of composite product Security Target (ASE_COMP)	106
11.4.1	Evaluation of sub-activity (ASE_COMP.1)	106
11.5	Extended components definition (ASE_ECD)	111
11.5.1	Evaluation of sub-activity (ASE_ECD.1)	111
11.6	ST introduction (ASE_INT)	115
11.6.1	Evaluation of sub-activity (ASE_INT.1)	115
11.7	Security objectives (ASE_OBJ)	118
11.7.1	Evaluation of sub-activity (ASE_OBJ.1)	118
11.7.2	Evaluation of sub-activity (ASE_OBJ.2)	120
11.8	Security requirements (ASE_REQ)	122
11.8.1	Evaluation of sub-activity (ASE_REQ.1)	122
11.8.2	Evaluation of sub-activity (ASE_REQ.2)	129
11.9	Security problem definition (ASE_SPD)	135
11.9.1	Evaluation of sub-activity (ASE_SPD.1)	135
11.10	TOE summary specification (ASE_TSS)	136
11.10.1	Evaluation of sub-activity (ASE_TSS.1)	136
11.10.2	Evaluation of sub-activity (ASE_TSS.2)	137
12	Class ADV Development	138
12.1	Introduction	138
12.2	Application notes	139
12.2.1	Composition	139
12.3	Security architecture (ADV_ARC)	140
12.3.1	Evaluation of sub-activity (ADV_ARC.1)	140
12.4	Composite design compliance (ADV_COMP)	144
12.4.1	Evaluation of sub-activity (ADV_COMP.1)	144
12.5	Functional specification (ADV_FSP)	146
12.5.1	Evaluation of sub-activity (ADV_FSP.1)	146
12.5.2	Evaluation of sub-activity (ADV_FSP.2)	149
12.5.3	Evaluation of sub-activity (ADV_FSP.3)	154
12.5.4	Evaluation of sub-activity (ADV_FSP.4)	159
12.5.5	Evaluation of sub-activity (ADV_FSP.5)	165
12.6	Implementation representation (ADV_IMP)	171
12.6.1	Evaluation of sub-activity (ADV_IMP.1)	171
12.6.2	Evaluation of sub-activity (ADV_IMP.2)	173
12.7	TSF internals (ADV_INT)	176
12.7.1	Evaluation of sub-activity (ADV_INT.1)	176
12.7.2	Evaluation of sub-activity (ADV_INT.2)	178

ISO/IEC DIS 18045:2024(en)

12.7.3	Evaluation of sub-activity (ADV_INT.3)	180
12.8	Formal TSF model (ADV_SPM)	183
12.8.1	Evaluation of sub-activity (ADV_SPM.1)	183
12.9	TOE design (ADV_TDS)	189
12.9.1	Evaluation of sub-activity (ADV_TDS.1)	189
12.9.2	Evaluation of sub-activity (ADV_TDS.2)	193
12.9.3	Evaluation of sub-activity (ADV_TDS.3)	198
12.9.4	Evaluation of sub-activity (ADV_TDS.4)	207
12.9.5	Evaluation of sub-activity (ADV_TDS.5)	216
13	Class AGD Guidance documents	223
13.1	Introduction	223
13.2	Application notes	224
13.3	Operational user guidance (AGD_OPE)	224
13.3.1	Evaluation of sub-activity (AGD_OPE.1)	224
13.4	Preparative procedures (AGD_PRE)	227
13.4.1	Evaluation of sub-activity (AGD_PRE.1)	227
14	Class ALC Life-cycle support	229
14.1	Introduction	229
14.2	Application notes	229
14.2.1	Composition	229
14.3	CM capabilities (ALC_CMC)	230
14.3.1	Evaluation of sub-activity (ALC_CMC.1)	230
14.3.2	Evaluation of sub-activity (ALC_CMC.2)	231
14.3.3	Evaluation of sub-activity (ALC_CMC.3)	232
14.3.4	Evaluation of sub-activity (ALC_CMC.4)	236
14.3.5	Evaluation of sub-activity (ALC_CMC.5)	242
14.4	CM scope (ALC_CMS)	249
14.4.1	Evaluation of sub-activity (ALC_CMS.1)	249
14.4.2	Evaluation of sub-activity (ALC_CMS.2)	250
14.4.3	Evaluation of sub-activity (ALC_CMS.3)	251
14.4.4	Evaluation of sub-activity (ALC_CMS.4)	252
14.4.5	Evaluation of sub-activity (ALC_CMS.5)	253
14.5	Integration of composition parts and consistency check of delivery procedures (ALC_COMP)	254
14.5.1	Evaluation of sub-activity (ALC_COMP.1)	254
14.6	Delivery (ALC_DEL)	257
14.6.1	Evaluation of sub-activity (ALC_DEL.1)	257
14.7	Developer environment security (ALC_DVS)	258
14.7.1	Evaluation of sub-activity (ALC_DVS.1)	258
14.7.2	Evaluation of sub-activity (ALC_DVS.2)	260
14.8	Flaw remediation (ALC_FLR)	263
14.8.1	Evaluation of sub-activity (ALC_FLR.1)	263
14.8.2	Evaluation of sub-activity (ALC_FLR.2)	265
14.8.3	Evaluation of sub-activity (ALC_FLR.3)	269
14.9	Development life-cycle definition (ALC_LCD)	274
14.9.1	Evaluation of sub-activity (ALC_LCD.1)	274
14.9.2	Evaluation of sub-activity (ALC_LCD.2)	275
14.10	Tools and techniques (ALC_TAT)	278
14.10.1	Evaluation of sub-activity (ALC_TAT.1)	278
14.10.2	Evaluation of sub-activity (ALC_TAT.2)	280
14.10.3	Evaluation of sub-activity (ALC_TAT.3)	283
14.11	TOE development artefacts (ALC_TDA)	285
14.11.1	Evaluation of sub-activity (ALC_TDA.1)	285
14.11.2	Evaluation of sub-activity (ALC_TDA.2)	289
14.11.3	Evaluation of sub-activity (ALC_TDA.3)	293
15	Class ATE Tests	297
15.1	Introduction	297

ISO/IEC DIS 18045:2024(en)

15.2	Application notes.....	297
15.2.1	Understanding the expected behaviour of the TOE.....	298
15.2.2	Testing vs. alternate approaches to verify the expected behaviour of functionality.....	298
15.2.3	Verifying the adequacy of tests.....	299
15.2.4	Composition.....	299
15.3	Composite functional testing (ATE_COMP).....	299
15.3.1	Evaluation of sub-activity (ATE_COMP.1).....	299
15.4	Coverage (ATE_COV).....	301
15.4.1	Evaluation of sub-activity (ATE_COV.1).....	301
15.4.2	Evaluation of sub-activity (ATE_COV.2).....	301
15.4.3	Evaluation of sub-activity (ATE_COV.3).....	303
15.5	Depth (ATE_DPT).....	305
15.5.1	Evaluation of sub-activity (ATE_DPT.1).....	305
15.5.2	Evaluation of sub-activity (ATE_DPT.2).....	307
15.5.3	Evaluation of sub-activity (ATE_DPT.3).....	310
15.6	Functional tests (ATE_FUN).....	312
15.6.1	Evaluation of sub-activity (ATE_FUN.1).....	312
15.6.2	Evaluation of sub-activity (ATE_FUN.2).....	315
15.7	Independent testing (ATE_IND).....	319
15.7.1	Evaluation of sub-activity (ATE_IND.1).....	319
15.7.2	Evaluation of sub-activity (ATE_IND.2).....	323
16	Class AVA Vulnerability assessment.....	327
16.1	Introduction.....	327
16.2	Application notes.....	328
16.2.1	Composition.....	328
16.3	Composite vulnerability assessment (AVA_COMP).....	328
16.3.1	Evaluation of sub-activity (AVA_COMP.1).....	328
16.4	Vulnerability analysis (AVA_VAN).....	330
16.4.1	Evaluation of sub-activity (AVA_VAN.1).....	330
16.4.2	Evaluation of sub-activity (AVA_VAN.2).....	335
16.4.3	Evaluation of sub-activity (AVA_VAN.3).....	342
16.4.4	Evaluation of sub-activity (AVA_VAN.4).....	350
16.4.5	Evaluation of sub-activity (AVA_VAN.5).....	357
17	Class ACO Composition.....	365
17.1	Introduction.....	365
17.2	Application notes.....	365
17.3	Composition rationale (ACO_COR).....	366
17.3.1	Evaluation of sub-activity (ACO_COR.1).....	366
17.4	Composed TOE testing (ACO_CTT).....	371
17.4.1	Evaluation of sub-activity (ACO_CTT.1).....	371
17.4.2	Evaluation of sub-activity (ACO_CTT.2).....	374
17.5	Development evidence (ACO_DEV).....	378
17.5.1	Evaluation of sub-activity (ACO_DEV.1).....	378
17.5.2	Evaluation of sub-activity (ACO_DEV.2).....	379
17.5.3	Evaluation of sub-activity (ACO_DEV.3).....	381
17.6	Reliance of dependent component (ACO_REL).....	384
17.6.1	Evaluation of sub-activity (ACO_REL.1).....	384
17.6.2	Evaluation of sub-activity (ACO_REL.2).....	386
17.7	Composition vulnerability analysis (ACO_VUL).....	388
17.7.1	Evaluation of sub-activity (ACO_VUL.1).....	388
17.7.2	Evaluation of sub-activity (ACO_VUL.2).....	391
17.7.3	Evaluation of sub-activity (ACO_VUL.3).....	395
	Annex A (informative) General evaluation guidance.....	399
	Annex B (informative) Vulnerability assessment (AVA).....	408
	Annex C (informative) Evaluation techniques and tools.....	428

ISO/IEC DIS 18045:2024(en)

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: [oSIST prEN ISO/IEC 18045:2024](https://standards.iso.org/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-18045-2024)

— xxx xxxxxxxx xxx xxx

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.

ISO/IEC DIS 18045:2024(en)**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 National Institute of Standards and Technology

[oSIST prEN ISO/IEC 18045:2024](https://standards.iteh.ai/catalog/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-18045-2024)

<https://standards.iteh.ai/catalog/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-18045-2024>

ISO/IEC DIS 18045:2024(en)

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.

iTeh Standards (<https://standards.iteh.ai>) Document Preview

[oSIST prEN ISO/IEC 18045:2024](https://standards.iteh.ai/catalog/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-18045-2024)

<https://standards.iteh.ai/catalog/standards/sist/645bc281-965a-486f-ab97-2ac1d1816c5c/osist-pren-iso-iec-18045-2024>

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.

ISO/IEC DIS 18045:2024(en)

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.