



SLOVENSKI STANDARD
oSIST prEN ISO/IEC 18045:2020
01-januar-2020

Informacijska tehnologija - Varnostne tehnike - Metodologija za varnostno vrednotenje IT (ISO/IEC 18045:2008)

Information technology - Security techniques - Methodology for IT security evaluation (ISO/IEC 18045:2008)

Informationstechnik - Sicherheitstechniken - Methodik für die Bewertung der IT-Sicherheit (ISO/IEC 18045:2008)

Technologies de l'information - Techniques de sécurité - Méthodologie pour l'évaluation de sécurité TI (ISO/IEC 18045:2008)

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

ICS:

35.030 Informacijska varnost IT Security

oSIST prEN ISO/IEC 18045:2020 en

INTERNATIONAL STANDARD

ISO/IEC 18045

Second edition
2008-08-15

Corrected version
2014-01-15

Information technology — Security techniques — Methodology for IT security evaluation

*Technologies de l'information — Techniques de sécurité —
Méthodologie pour l'évaluation de sécurité TI*

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[SIST EN ISO/IEC 18045:2020](https://standards.iteh.ai/catalog/standards/sist/15a8bde9-8779-441a-a2f9-db9582f28fb0/sist-en-iso-iec-18045-2020)

[https://standards.iteh.ai/catalog/standards/sist/15a8bde9-8779-441a-a2f9-
db9582f28fb0/sist-en-iso-iec-18045-2020](https://standards.iteh.ai/catalog/standards/sist/15a8bde9-8779-441a-a2f9-db9582f28fb0/sist-en-iso-iec-18045-2020)

Reference number
ISO/IEC 18045:2008(E)



iTeh STANDARD PREVIEW (standards.iteh.ai)

SIST EN ISO/IEC 18045:2020

<https://standards.iteh.ai/catalog/standards/sist/15a8bde9-8779-441a-a2f9-db9582f28fb0/sist-en-iso-iec-18045-2020>



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword	vii
Introduction.....	ix
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Symbols and abbreviated terms	3
5 Overview.....	3
5.1 Organisation of this International Standard	3
6 Document Conventions	3
6.1 Terminology	3
6.2 Verb usage	3
6.3 General evaluation guidance	4
6.4 Relationship between ISO/IEC 15408 and ISO/IEC 18045 structures.....	4
7 Evaluation process and related tasks	5
7.1 Introduction.....	5
7.2 Evaluation process overview	5
7.2.1 Objectives	5
7.2.2 Responsibilities of the roles	5
7.2.3 Relationship of roles	6
7.2.4 General evaluation model.....	6
7.2.5 Evaluator verdicts	6
7.3 Evaluation input task	8
7.3.1 Objectives	8
7.3.2 Application notes	8
7.3.3 Management of evaluation evidence sub-task.....	8
7.4 Evaluation sub-activities	9
7.5 Evaluation output task.....	9
7.5.1 Objectives	9
7.5.2 Management of evaluation outputs	9
7.5.3 Application notes	10
7.5.4 Write OR sub-task	10
7.5.5 Write ETR sub-task.....	10
8 Class APE: Protection Profile evaluation	15
8.1 Introduction.....	15
8.2 Application notes	16
8.2.1 Re-using the evaluation results of certified PPs.....	16
8.3 PP introduction (APE_INT)	16
8.3.1 Evaluation of sub-activity (APE_INT.1)	16
8.4 Conformance claims (APE_CCL).....	17
8.4.1 Evaluation of sub-activity (APE_CCL.1).....	17
8.5 Security problem definition (APE_SPD).....	24
8.5.1 Evaluation of sub-activity (APE_SPD.1).....	24
8.6 Security objectives (APE_OBJ)	25
8.6.1 Evaluation of sub-activity (APE_OBJ.1).....	25
8.6.2 Evaluation of sub-activity (APE_OBJ.2).....	25
8.7 Extended components definition (APE_ECD)	28
8.7.1 Evaluation of sub-activity (APE_ECD.1)	28
8.8 Security requirements (APE_REQ).....	31

ISO/IEC 18045:2008(E)

8.8.1	Evaluation of sub-activity (APE_REQ.1)	31
8.8.2	Evaluation of sub-activity (APE_REQ.2)	35
9	Class ASE: Security Target evaluation	39
9.1	Introduction	39
9.2	Application notes	39
9.2.1	Re-using the evaluation results of certified PPs	39
9.3	ST introduction (ASE_INT)	39
9.3.1	Evaluation of sub-activity (ASE_INT.1)	39
9.4	Conformance claims (ASE_CCL)	42
9.4.1	Evaluation of sub-activity (ASE_CCL.1)	42
9.5	Security problem definition (ASE_SPD)	49
9.5.1	Evaluation of sub-activity (ASE_SPD.1)	49
9.6	Security objectives (ASE_OBJ)	51
9.6.1	Evaluation of sub-activity (ASE_OBJ.1)	51
9.6.2	Evaluation of sub-activity (ASE_OBJ.2)	51
9.7	Extended components definition (ASE_ECD)	53
9.7.1	Evaluation of sub-activity (ASE_ECD.1)	53
9.8	Security requirements (ASE_REQ)	57
9.8.1	Evaluation of sub-activity (ASE_REQ.1)	57
9.8.2	Evaluation of sub-activity (ASE_REQ.2)	60
9.9	TOE summary specification (ASE_TSS)	64
9.9.1	Evaluation of sub-activity (ASE_TSS.1)	64
9.9.2	Evaluation of sub-activity (ASE_TSS.2)	65
10	Class ADV: Development	67
10.1	Introduction	67
10.2	Application notes	67
10.3	Security Architecture (ADV_ARC)	67
10.3.1	Evaluation of sub-activity (ADV_ARC.1)	67
10.4	Functional specification (ADV_FSP)	72
10.4.1	Evaluation of sub-activity (ADV_FSP.1)	72
10.4.2	Evaluation of sub-activity (ADV_FSP.2)	75
10.4.3	Evaluation of sub-activity (ADV_FSP.3)	79
10.4.4	Evaluation of sub-activity (ADV_FSP.4)	84
10.4.5	Evaluation of sub-activity (ADV_FSP.5)	89
10.4.6	Evaluation of sub-activity (ADV_FSP.6)	94
10.5	Implementation representation (ADV_IMP)	95
10.5.1	Evaluation of sub-activity (ADV_IMP.1)	95
10.5.2	Evaluation of sub-activity (ADV_IMP.2)	97
10.6	TSF internals (ADV_INT)	97
10.6.1	Evaluation of sub-activity (ADV_INT.1)	97
10.6.2	Evaluation of sub-activity (ADV_INT.2)	99
10.6.3	Evaluation of sub-activity (ADV_INT.3)	101
10.7	Security policy modelling (ADV_SPM)	101
10.7.1	Evaluation of sub-activity (ADV_SPM.1)	101
10.8	TOE design (ADV_TDS)	101
10.8.1	Evaluation of sub-activity (ADV_TDS.1)	101
10.8.2	Evaluation of sub-activity (ADV_TDS.2)	105
10.8.3	Evaluation of sub-activity (ADV_TDS.3)	109
10.8.4	Evaluation of sub-activity (ADV_TDS.4)	118
10.8.5	Evaluation of sub-activity (ADV_TDS.5)	126
10.8.6	Evaluation of sub-activity (ADV_TDS.6)	126
11	Class AGD: Guidance documents	127
11.1	Introduction	127
11.2	Application notes	127
11.3	Operational user guidance (AGD_OPE)	127
11.3.1	Evaluation of sub-activity (AGD_OPE.1)	127
11.4	Preparative procedures (AGD_PRE)	130
11.4.1	Evaluation of sub-activity (AGD_PRE.1)	130

12	Class ALC: Life-cycle support	131
12.1	Introduction.....	131
12.2	CM capabilities (ALC_CMC)	132
12.2.1	Evaluation of sub-activity (ALC_CMC.1).....	132
12.2.2	Evaluation of sub-activity (ALC_CMC.2).....	133
12.2.3	Evaluation of sub-activity (ALC_CMC.3).....	135
12.2.4	Evaluation of sub-activity (ALC_CMC.4).....	138
12.2.5	Evaluation of sub-activity (ALC_CMC.5).....	143
12.3	CM scope (ALC_CMS).....	150
12.3.1	Evaluation of sub-activity (ALC_CMS.1).....	150
12.3.2	Evaluation of sub-activity (ALC_CMS.2).....	151
12.3.3	Evaluation of sub-activity (ALC_CMS.3).....	152
12.3.4	Evaluation of sub-activity (ALC_CMS.4).....	153
12.3.5	Evaluation of sub-activity (ALC_CMS.5).....	154
12.4	Delivery (ALC_DEL).....	155
12.4.1	Evaluation of sub-activity (ALC_DEL.1).....	155
12.5	Development security (ALC_DVS).....	156
12.5.1	Evaluation of sub-activity (ALC_DVS.1).....	156
12.5.2	Evaluation of sub-activity (ALC_DVS.2).....	158
12.6	Flaw remediation (ALC_FLR)	161
12.6.1	Evaluation of sub-activity (ALC_FLR.1).....	161
12.6.2	Evaluation of sub-activity (ALC_FLR.2).....	163
12.6.3	Evaluation of sub-activity (ALC_FLR.3).....	167
12.7	Life-cycle definition (ALC_LCD)	171
12.7.1	Evaluation of sub-activity (ALC_LCD.1).....	171
12.7.2	Evaluation of sub-activity (ALC_LCD.2).....	172
12.8	Tools and techniques (ALC_TAT).....	174
12.8.1	Evaluation of sub-activity (ALC_TAT.1).....	174
12.8.2	Evaluation of sub-activity (ALC_TAT.2).....	176
12.8.3	Evaluation of sub-activity (ALC_TAT.3).....	178
13	Class ATE: Tests	181
13.1	Introduction.....	181
13.2	Application notes	181
13.2.1	Understanding the expected behaviour of the TOE	181
13.2.2	Testing vs. alternate approaches to verify the expected behaviour of functionality	182
13.2.3	Verifying the adequacy of tests	182
13.3	Coverage (ATE_COV).....	183
13.3.1	Evaluation of sub-activity (ATE_COV.1)	183
13.3.2	Evaluation of sub-activity (ATE_COV.2)	183
13.3.3	Evaluation of sub-activity (ATE_COV.3)	184
13.4	Depth (ATE_DPT).....	185
13.4.1	Evaluation of sub-activity (ATE_DPT.1)	185
13.4.2	Evaluation of sub-activity (ATE_DPT.2).....	187
13.4.3	Evaluation of sub-activity (ATE_DPT.3).....	189
13.4.4	Evaluation of sub-activity (ATE_DPT.4).....	192
13.5	Functional tests (ATE_FUN).....	192
13.5.1	Evaluation of sub-activity (ATE_FUN.1).....	192
13.5.2	Evaluation of sub-activity (ATE_FUN.2).....	195
13.6	Independent testing (ATE_IND)	195
13.6.1	Evaluation of sub-activity (ATE_IND.1).....	195
13.6.2	Evaluation of sub-activity (ATE_IND.2).....	198
13.6.3	Evaluation of sub-activity (ATE_IND.3).....	203
14	Class AVA: Vulnerability assessment	203
14.1	Introduction.....	203
14.2	Vulnerability analysis (AVA_VAN).....	204
14.2.1	Evaluation of sub-activity (AVA_VAN.1)	204
14.2.2	Evaluation of sub-activity (AVA_VAN.2).....	208
14.2.3	Evaluation of sub-activity (AVA_VAN.3).....	215
14.2.4	Evaluation of sub-activity (AVA_VAN.4).....	222

ISO/IEC 18045:2008(E)

14.2.5	Evaluation of sub-activity (AVA_VAN.5)	230
15	Class ACO: Composition	230
15.1	Introduction	230
15.2	Application notes	230
15.3	Composition rationale (ACO_COR)	231
15.3.1	Evaluation of sub-activity (ACO_COR.1)	231
15.4	Development evidence (ACO_DEV)	236
15.4.1	Evaluation of sub-activity (ACO_DEV.1)	236
15.4.2	Evaluation of sub-activity (ACO_DEV.2)	237
15.4.3	Evaluation of sub-activity (ACO_DEV.3)	239
15.5	Reliance of dependent component (ACO_REL)	242
15.5.1	Evaluation of sub-activity (ACO_REL.1)	242
15.5.2	Evaluation of sub-activity (ACO_REL.2)	244
15.6	Composed TOE testing (ACO_CTT)	246
15.6.1	Evaluation of sub-activity (ACO_CTT.1)	246
15.6.2	Evaluation of sub-activity (ACO_CTT.2)	248
15.7	Composition vulnerability analysis (ACO_VUL)	252
15.7.1	Evaluation of sub-activity (ACO_VUL.1)	252
15.7.2	Evaluation of sub-activity (ACO_VUL.2)	254
15.7.3	Evaluation of sub-activity (ACO_VUL.3)	258
Annex A	(informative) General evaluation guidance	262
A.1	Objectives	262
A.2	Sampling	262
A.3	Dependencies	264
A.3.1	Dependencies between activities	264
A.3.2	Dependencies between sub-activities	264
A.3.3	Dependencies between actions	264
A.4	Site Visits	264
A.4.1	Introduction	264
A.4.2	General Approach	265
A.4.3	Orientation Guide for the Preparation of the Check List	266
A.4.4	Example of a checklist	267
A.5	Scheme Responsibilities	269
Annex B	(informative) Vulnerability Assessment (AVA)	271
B.1	What is Vulnerability Analysis	271
B.2	Evaluator construction of a Vulnerability Analysis	271
B.2.1	Generic vulnerability guidance	272
B.2.2	Identification of Potential Vulnerabilities	279
B.3	When attack potential is used	281
B.3.1	Developer	281
B.3.2	Evaluator	282
B.4	Calculating attack potential	283
B.4.1	Application of attack potential	283
B.4.2	Characterising attack potential	283
B.5	Example calculation for direct attack	289

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

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.

ISO/IEC 18045 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology, Subcommittee SC 27, IT Security techniques*. The identical text of ISO/IEC 18045 is published by the Common Criteria Project Sponsoring Organisations as *Common Methodology for Information Technology Security Evaluation*. The common XML source for both publications can be found at <http://www.commoncriteriaportal.org/cc/>.

This second edition cancels and replaces the first edition (ISO/IEC 18045:2005), which has been technically revised.

This second corrected version of ISO/IEC 18045:2008 incorporates miscellaneous editorial corrections related to the following:

- consistency with the corrected versions of ISO/IEC 15408-3:2008 and ISO/IEC 15408-1:2009;
- APE_CCL and ASE_CCL, APE_SPD and ASE_SPD, AGD_PRE, ALC_CMC, ALC_DVS, ADV_TDS, ASE_TSS, AVA_VAN, and ADV_FSP.

ISO/IEC 18045:2008(E)**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, version 3.1 (called CEM 3.1), they hereby grant non-exclusive license to ISO/IEC to use CEM 3.1 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 3.1 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;
France:	Direction Centrale 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;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

[SIST EN ISO/IEC 18045:2020](https://standards.iteh.ai/catalog/standards/sist/15a8bde9-8779-441a-a2f9-db9582f28fb0/sist-en-iso-iec-18045-2020)

<https://standards.iteh.ai/catalog/standards/sist/15a8bde9-8779-441a-a2f9-db9582f28fb0/sist-en-iso-iec-18045-2020>

Introduction

The target audience for this International Standard is primarily evaluators applying ISO/IEC 15408 and certifiers confirming evaluator actions; evaluation sponsors, developers, PP/ST authors and other parties interested in IT security may be a secondary audience.

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

iTeh STANDARD PREVIEW (standards.iteh.ai)

[SIST EN ISO/IEC 18045:2020](https://standards.iteh.ai/catalog/standards/sist/15a8bde9-8779-441a-a2f9-db9582f28fb0/sist-en-iso-iec-18045-2020)

<https://standards.iteh.ai/catalog/standards/sist/15a8bde9-8779-441a-a2f9-db9582f28fb0/sist-en-iso-iec-18045-2020>

Information technology — Security techniques — Methodology for IT security evaluation

1 Scope

This International Standard is a companion document to the “Evaluation criteria for IT security”, ISO/IEC 15408. This International Standard defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.

This International Standard does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

2 Normative references

The following referenced documents are indispensable for the application 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 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE Terms which are presented in bold-faced type are themselves defined in this Subclause.

3.1

action

evaluator action element of ISO/IEC 15408-3

NOTE These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.

3.2

activity

application of an assurance class of ISO/IEC 15408-3

3.3

check

generate a **verdict** by a simple comparison

NOTE Evaluator expertise is not required. The statement that uses this verb describes what is mapped.

3.4

evaluation deliverable

any resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities

3.5

evaluation evidence

tangible **evaluation deliverable**

ISO/IEC 18045:2008(E)

3.6
evaluation technical report
report that documents the **overall verdict** and its justification, produced by the evaluator and submitted to an evaluation authority

3.7
examine
generate a **verdict** by analysis using evaluator expertise

NOTE The statement that uses this verb identifies what is analysed and the properties for which it is analysed.

3.8
interpretation
clarification or amplification of an ISO/IEC 15408, ISO/IEC 18045 or **scheme** requirement

3.9
methodology
system of principles, procedures and processes applied to IT security evaluations

3.10
observation report
report written by the evaluator requesting a clarification or identifying a problem during the evaluation

3.11
overall verdict
pass or fail statement issued by an evaluator with respect to the result of an evaluation

3.12
oversight verdict
statement issued by an evaluation authority confirming or rejecting an *overall verdict* based on the results of evaluation oversight activities

3.13
record
retain a written description of procedures, events, observations, insights and results in sufficient detail to enable the work performed during the evaluation to be reconstructed at a later time

3.14
report
include evaluation results and supporting material in the **Evaluation Technical Report** or an **Observation Report**

3.15
scheme
set of rules, established by an evaluation authority, defining the evaluation environment, including criteria and **methodology** required to conduct IT security evaluations

3.16
sub-activity
application of an assurance component of ISO/IEC 15408-3

NOTE Assurance families are not explicitly addressed in this International Standard because evaluations are conducted on a single assurance component from an assurance family.

3.17
tracing
simple directional relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second

3.18**verdict**

pass, fail or inconclusive statement issued by an evaluator with respect to an ISO/IEC 15408 evaluator action element, assurance component, or class

NOTE Also see **overall verdict**.

3.19**work unit**

most granular level of evaluation work

NOTE Each evaluation methodology action comprises one or more work units, which are grouped within the evaluation methodology action by ISO/IEC 15408 content and presentation of evidence or developer action element. The work units are presented in this International Standard in the same order as ISO/IEC 15408 elements from which they are derived. Work units are identified in the left margin by a symbol such as ALC_TAT.1-2. In this symbol, the string *ALC_TAT.1* indicates ISO/IEC 15408 component (i.e. this International Standard sub-activity), and the final digit (2) indicates that this is the second work unit in the ALC_TAT.1 sub-activity.

4 Symbols and abbreviated terms

ETR Evaluation Technical Report

OR Observation Report

5 Overview**5.1 Organisation of this International Standard**

Clause 6 defines the conventions used in this International Standard.

Clause 7 describes general evaluation tasks with no verdicts associated with them as they do not map to ISO/IEC 15408 evaluator action elements.

Clause 8 addresses the work necessary for reaching an evaluation result on a PP.

Clauses 9 to 15 define the evaluation activities, organised by Assurance Classes.

Annex A covers the basic evaluation techniques used to provide technical evidence of evaluation results.

Annex B provides an explanation of the Vulnerability Analysis criteria and examples of their application

6 Document Conventions**6.1 Terminology**

Unlike ISO/IEC 15408, where each element maintains the last digit of its identifying symbol for all components within the family, this International Standard may introduce new work units when an ISO/IEC 15408 evaluator action element changes from sub-activity to sub-activity; as a result, the last digit of the work unit's identifying symbol may change although the work unit remains unchanged.

Any methodology-specific evaluation work required that is not derived directly from ISO/IEC 15408 requirements is termed *task* or *sub-task*.

6.2 Verb usage

All work unit and sub-task verbs are preceded by the auxiliary verb *shall* and by presenting both the verb and the *shall* in **bold italic** type face. The auxiliary verb *shall* is used only when the provided text is mandatory and