ICS 35.020, 35.040 SLOVENSKÁ TECHNICKÁ NORMA Január 2024

STN	**Informačná bezpečnosť, kybernetická bezpečnosť a ochrana súkromia Kritériá na hodnotenie bezpečnosti IT Metodika na hodnotenie bezpečnosti IT (ISO/IEC 18045: 2022)**	**STN EN ISO/IEC 18045** 97 4111

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation (ISO/IEC 18045:2022)

Táto norma obsahuje anglickú verziu európskej normy.
This standard includes the English version of the European Standard.

Táto norma bola oznámená vo Vestníku ÚNMS SR č. 12/23

Obsahuje: EN ISO/IEC 18045:2023, ISO/IEC 18045:2022

Oznámením tejto normy sa ruší
STN EN ISO/IEC 18045 (36 9777) zo septembra 2020

137929

Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky, 2024
Slovenská technická norma a technická normalizačná informácia je chránená zákonom č. 60/2018 Z. z. o technickej normalizácii v znení neskorších predpisov.

EUROPEAN STANDARD

NORME EUROPÉENNE

EUROPÄISCHE NORM

EN ISO/IEC 18045

November 2023

ICS 35.030

Supersedes EN ISO/IEC 18045:2020

English version

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation (ISO/IEC 18045:2022)

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 18045:2022)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Evaluationskriterien für IT-Sicherheit - Methodik für die Bewertung der IT-Sicherheit (ISO/IEC 18045:2022)

This European Standard was approved by CEN on 29 October 2023.

CEN and CENELEC members are bound to comply with the CEN/CENELEC Internal Regulations which stipulate the conditions for giving this European Standard the status of a national standard without any alteration. Up-to-date lists and bibliographical references concerning such national standards may be obtained on application to the CEN-CENELEC Management Centre or to any CEN and CENELEC member.

This European Standard exists in three official versions (English, French, German). A version in any other language made by translation under the responsibility of a CEN and CENELEC member into its own language and notified to the CEN-CENELEC Management Centre has the same status as the official versions.

CEN and CENELEC members are the national standards bodies and national electrotechnical committees of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

CEN-CENELEC Management Centre:
Rue de la Science 23, B-1040 Brussels

© 2023 CEN/CENELEC All rights of exploitation in any form and by any means reserved worldwide for CEN national Members and for CENELEC Members.

Contents

Page

European foreword..... 3

European foreword

The text of ISO/IEC 18045:2022 has been prepared by Technical Committee ISO/IEC JTC 1 "Information technology" of the International Organization for Standardization (ISO) and has been taken over as EN ISO/IEC 18045:2023 by Technical Committee CEN-CENELEC/ JTC 13 "Cybersecurity and Data Protection" the secretariat of which is held by DIN.

This European Standard shall be given the status of a national standard, either by publication of an identical text or by endorsement, at the latest by May 2024, and conflicting national standards shall be withdrawn at the latest by May 2024.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN-CENELEC shall not be held responsible for identifying any or all such patent rights.

This document supersedes EN ISO/IEC 18045:2020.

Any feedback and questions on this document should be directed to the users' national standards body. A complete listing of these bodies can be found on the CEN and CENELEC websites.

According to the CEN-CENELEC Internal Regulations, the national standards organizations of the following countries are bound to implement this European Standard: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Endorsement notice

The text of ISO/IEC 18045:2022 has been approved by CEN-CENELEC as EN ISO/IEC 18045:2023 without any modification.

INTERNATIONAL STANDARD

ISO/IEC 18045

Third edition
2022-08

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

Reference number
ISO/IEC 18045:2022(E)

© ISO/IEC 2022

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
Website: www.iso.org

Published in Switzerland

Table of Contents

LIST OF FIGURES ... **ix**

LIST OF TABLES ... **x**

FOREWORD ... **xi**

INTRODUCTION ... **xii**

1 SCOPE ... **1**

2 NORMATIVE REFERENCES ... **1**

3 TERMS AND DEFINITIONS ... **1**

4 ABBREVIATED TERMS ... **4**

5 TERMINOLOGY ... **4**

6 VERB USAGE ... **4**

7 GENERAL EVALUATION GUIDANCE ... **5**

8 RELATIONSHIP BETWEEN THE ISO/IEC 15408 SERIES AND ISO/IEC 18045 STRUCTURES ... **5**

9 EVALUATION PROCESS AND RELATED TASKS ... **5**

9.1 GENERAL ... 5
9.2 EVALUATION PROCESS OVERVIEW ... 6
9.2.1 Objectives ... *6*
9.2.2 Responsibilities of the roles ... *6*
9.2.3 Relationship of roles ... *6*
9.2.4 General evaluation model ... *7*
9.2.5 Evaluator verdicts ... *7*
9.3 EVALUATION INPUT TASK ... 9
9.3.1 Objectives ... *9*
9.3.2 Application notes ... *9*
9.3.3 Management of evaluation evidence sub-task ... *10*
9.4 EVALUATION SUB-ACTIVITIES ... 10
9.5 EVALUATION OUTPUT TASK ... 10
9.5.1 Objectives ... *10*
9.5.2 Management of evaluation outputs ... *11*
9.5.3 Application notes ... *11*
9.5.4 Write OR sub-task ... *11*
9.5.5 Write ETR sub-task ... *11*

10 CLASS APE: PROTECTION PROFILE EVALUATION ... **19**

10.1 GENERAL ... 19
10.2 RE-USING THE EVALUATION RESULTS OF CERTIFIED PPS ... 19
10.3 PP INTRODUCTION (APE_INT) ... 20
10.3.1 Evaluation of sub-activity (APE_INT.1) ... *20*
10.4 CONFORMANCE CLAIMS (APE_CCL) ... 21
10.4.1 Evaluation of sub-activity (APE_CCL.1) ... *21*
10.5 SECURITY PROBLEM DEFINITION (APE_SPD) ... 31
10.5.1 Evaluation of sub-activity (APE_SPD.1) ... *31*
10.6 SECURITY OBJECTIVES (APE_OBJ) ... 32
10.6.1 Evaluation of sub-activity (APE_OBJ.1) ... *32*
10.6.2 Evaluation of sub-activity (APE_OBJ.2) ... *33*
10.7 EXTENDED COMPONENTS DEFINITION (APE_ECD) ... 36
10.7.1 Evaluation of sub-activity (APE_ECD.1) ... *36*

© ISO/IEC 2022 – All rights reserved

10.8 SECURITY REQUIREMENTS (APE_REQ) 40
10.8.1 Evaluation of sub-activity (APE_REQ.1) *40*
10.8.2 Evaluation of sub-activity (APE_REQ.2) *45*

11 CLASS ACE: PROTECTION PROFILE CONFIGURATION EVALUATION 49

11.1 GENERAL 49
11.2 PP-MODULE INTRODUCTION (ACE_INT) 51
11.2.1 Evaluation of sub-activity (ACE_INT.1) *51*
11.3 PP-MODULE CONFORMANCE CLAIMS (ACE_CCL) 53
11.3.1 Evaluation of sub-activity (ACE_CCL.1) *53*
11.4 PP-MODULE SECURITY PROBLEM DEFINITION (ACE_SPD) 58
11.4.1 Evaluation of sub-activity (ACE_SPD.1) *58*
11.5 PP-MODULE SECURITY OBJECTIVES (ACE_OBJ) 59
11.5.1 Evaluation of sub-activity (ACE_OBJ.1) *59*
11.5.2 Evaluation of sub-activity (ACE_OBJ.2) *60*
11.6 PP-MODULE EXTENDED COMPONENTS DEFINITION (ACE_ECD) 63
11.6.1 Evaluation of sub-activity (ACE_ECD.1) *63*
11.7 PP-MODULE SECURITY REQUIREMENTS (ACE_REQ) 67
11.7.1 Evaluation of sub-activity (ACE_REQ.1) *67*
11.7.2 Evaluation of sub-activity (ACE_REQ.2) *72*
11.8 PP-MODULE CONSISTENCY (ACE_MCO) 76
11.8.1 Evaluation of sub-activity (ACE_MCO.1) *76*
11.9 PP-CONFIGURATION CONSISTENCY (ACE_CCO) 79
11.9.1 Evaluation of sub-activity (ACE_CCO.1) *79*

12 CLASS ASE: SECURITY TARGET EVALUATION 87

12.1 GENERAL 87
12.2 APPLICATION NOTES 87
12.2.1 Re-using the evaluation results of certified PPs *87*
12.3 ST INTRODUCTION (ASE_INT) 88
12.3.1 Evaluation of sub-activity (ASE_INT.1) *88*
12.4 CONFORMANCE CLAIMS (ASE_CCL) 91
12.4.1 Evaluation of sub-activity (ASE_CCL.1) *91*
12.5 SECURITY PROBLEM DEFINITION (ASE_SPD) 105
12.5.1 Evaluation of sub-activity (ASE_SPD.1) *105*
12.6 SECURITY OBJECTIVES (ASE_OBJ) 106
12.6.1 Evaluation of sub-activity (ASE_OBJ.1) *106*
12.6.2 Evaluation of sub-activity (ASE_OBJ.2) *107*
12.7 EXTENDED COMPONENTS DEFINITION (ASE_ECD) 109
12.7.1 Evaluation of sub-activity (ASE_ECD.1) *109*
12.8 SECURITY REQUIREMENTS (ASE_REQ) 113
12.8.1 Evaluation of sub-activity (ASE_REQ.1) *113*
12.8.2 Evaluation of sub-activity (ASE_REQ.2) *119*
12.9 TOE SUMMARY SPECIFICATION (ASE_TSS) 124
12.9.1 Evaluation of sub-activity (ASE_TSS.1) *124*
12.9.2 Evaluation of sub-activity (ASE_TSS.2) *125*
12.10 CONSISTENCY OF COMPOSITE PRODUCT SECURITY TARGET (ASE_COMP) 127
12.10.1 General *127*
12.10.2 Evaluation of sub-activity (ASE_COMP.1) *127*

13 CLASS ADV: DEVELOPMENT 132

13.1 GENERAL 132
13.2 APPLICATION NOTES 132
13.3 SECURITY ARCHITECTURE (ADV_ARC) 133
13.3.1 Evaluation of sub-activity (ADV_ARC.1) *133*
13.4 FUNCTIONAL SPECIFICATION (ADV_FSP) 137
13.4.1 Evaluation of sub-activity (ADV_FSP.1) *137*
13.4.2 Evaluation of sub-activity (ADV_FSP.2) *140*

 © ISO/IEC 2022 – All rights reserved

13.4.3 Evaluation of sub-activity (ADV_FSP.3) ... 145
13.4.4 Evaluation of sub-activity (ADV_FSP.4) ... 150
13.4.5 Evaluation of sub-activity (ADV_FSP.5) ... 155
13.4.6 Evaluation of sub-activity (ADV_FSP.6) ... 161
13.5 IMPLEMENTATION REPRESENTATION (ADV_IMP) ... 161
13.5.1 Evaluation of sub-activity (ADV_IMP.1) ... 161
13.5.2 Evaluation of sub-activity (ADV_IMP.2) ... 164
13.6 TSF INTERNALS (ADV_INT) ... 166
13.6.1 Evaluation of sub-activity (ADV_INT.1) ... 166
13.6.2 Evaluation of sub-activity (ADV_INT.2) ... 169
13.6.3 Evaluation of sub-activity (ADV_INT.3) ... 171
13.7 FORMAL TSF MODEL (ADV_SPM) ... 173
13.7.1 Evaluation of sub-activity (ADV_SPM.1) ... 173
13.8 TOE DESIGN (ADV_TDS) ... 180
13.8.1 Evaluation of sub-activity (ADV_TDS.1) ... 180
13.8.2 Evaluation of sub-activity (ADV_TDS.2) ... 183
13.8.3 Evaluation of sub-activity (ADV_TDS.3) ... 188
13.8.4 Evaluation of sub-activity (ADV_TDS.4) ... 197
13.8.5 Evaluation of sub-activity (ADV_TDS.5) ... 206
13.8.6 Evaluation of sub-activity (ADV_TDS.6) ... 213
13.9 COMPOSITE DESIGN COMPLIANCE (ADV_COMP) ... 214
13.9.1 General ... 214
13.9.2 Evaluation of sub-activity (ADV_COMP.1) ... 214

14 CLASS AGD: GUIDANCE DOCUMENTS ... 216

14.1 GENERAL ... 216
14.2 APPLICATION NOTES ... 216
14.3 OPERATIONAL USER GUIDANCE (AGD_OPE) ... 216
14.3.1 Evaluation of sub-activity (AGD_OPE.1) ... 216
14.4 PREPARATIVE PROCEDURES (AGD_PRE) ... 219
14.4.1 Evaluation of sub-activity (AGD_PRE.1) ... 219

15 CLASS ALC: LIFE-CYCLE SUPPORT ... 221

15.1 GENERAL ... 221
15.2 CM CAPABILITIES (ALC_CMC) ... 222
15.2.1 Evaluation of sub-activity (ALC_CMC.1) ... 222
15.2.2 Evaluation of sub-activity (ALC_CMC.2) ... 223
15.2.3 Evaluation of sub-activity (ALC_CMC.3) ... 224
15.2.4 Evaluation of sub-activity (ALC_CMC.4) ... 228
15.2.5 Evaluation of sub-activity (ALC_CMC.5) ... 233
15.3 CM SCOPE (ALC_CMS) ... 240
15.3.1 Evaluation of sub-activity (ALC_CMS.1) ... 240
15.3.2 Evaluation of sub-activity (ALC_CMS.2) ... 241
15.3.3 Evaluation of sub-activity (ALC_CMS.3) ... 242
15.3.4 Evaluation of sub-activity (ALC_CMS.4) ... 243
15.3.5 Evaluation of sub-activity (ALC_CMS.5) ... 244
15.4 DELIVERY (ALC_DEL) ... 245
15.4.1 Evaluation of sub-activity (ALC_DEL.1) ... 245
15.5 DEVELOPMENT SECURITY (ALC_DVS) ... 247
15.5.1 Evaluation of sub-activity (ALC_DVS.1) ... 247
15.5.2 Evaluation of sub-activity (ALC_DVS.2) ... 249
15.6 FLAW REMEDIATION (ALC_FLR) ... 252
15.6.1 Evaluation of sub-activity (ALC_FLR.1) ... 252
15.6.2 Evaluation of sub-activity (ALC_FLR.2) ... 254
15.6.3 Evaluation of sub-activity (ALC_FLR.3) ... 257
15.7 LIFE-CYCLE DEFINITION (ALC_LCD) ... 262
15.7.1 Evaluation of sub-activity (ALC_LCD.1) ... 262
15.7.2 Evaluation of sub-activity (ALC_LCD.2) ... 263

© ISO/IEC 2022 – All rights reserved

15.8 TOE DEVELOPMENT ARTIFACTS (ALC_TDA) 265
15.8.1 Evaluation of sub-activity (ALC_TDA.1) 265
15.8.2 Evaluation of sub-activity (ALC_TDA.2) 268
15.8.3 Evaluation of sub-activity (ALC_TDA.3) 272
15.9 TOOLS AND TECHNIQUES (ALC_TAT) 276
15.9.1 Evaluation of sub-activity (ALC_TAT.1) 276
15.9.2 Evaluation of sub-activity (ALC_TAT.2) 278
15.9.3 Evaluation of sub-activity (ALC_TAT.3) 281
15.10 INTEGRATION OF COMPOSITION PARTS AND CONSISTENCY CHECK OF DELIVERY PROCEDURES (ALC_COMP) 284
15.10.1 General 284
15.10.2 Evaluation of sub-activity (ALC_COMP.1) 284

16 CLASS ATE: TESTS 286

16.1 GENERAL 286
16.2 APPLICATION NOTES 287
16.2.1 Understanding the expected behaviour of the TOE 287
16.2.2 Testing vs. alternate approaches to verify the expected behaviour of functionality 288
16.2.3 Verifying the adequacy of tests 288
16.3 COVERAGE (ATE_COV) 288
16.3.1 Evaluation of sub-activity (ATE_COV.1) 288
16.3.2 Evaluation of sub-activity (ATE_COV.2) 289
16.3.3 Evaluation of sub-activity (ATE_COV.3) 291
16.4 DEPTH (ATE_DPT) 293
16.4.1 Evaluation of sub-activity (ATE_DPT.1) 293
16.4.2 Evaluation of sub-activity (ATE_DPT.2) 295
16.4.3 Evaluation of sub-activity (ATE_DPT.3) 298
16.4.4 Evaluation of sub-activity (ATE_DPT.4) 300
16.5 FUNCTIONAL TESTS (ATE_FUN) 300
16.5.1 Evaluation of sub-activity (ATE_FUN.1) 300
16.5.2 Evaluation of sub-activity (ATE_FUN.2) 303
16.6 INDEPENDENT TESTING (ATE_IND) 307
16.6.1 Evaluation of sub-activity (ATE_IND.1) 307
16.6.2 Evaluation of sub-activity (ATE_IND.2) 311
16.6.3 Evaluation of sub-activity (ATE_IND.3) 316
16.7 COMPOSITE FUNCTIONAL TESTING (ATE_COMP) 316
16.7.1 General 316
16.7.2 Evaluation of sub-activity (ATE_COMP.1) 316

17 CLASS AVA: VULNERABILITY ASSESSMENT 317

17.1 GENERAL 317
17.2 VULNERABILITY ANALYSIS (AVA_VAN) 318
17.2.1 Evaluation of sub-activity (AVA_VAN.1) 318
17.2.2 Evaluation of sub-activity (AVA_VAN.2) 323
17.2.3 Evaluation of sub-activity (AVA_VAN.3) 329
17.2.4 Evaluation of sub-activity (AVA_VAN.4) 337
17.2.5 Evaluation of sub-activity (AVA_VAN.5) 345
17.3 COMPOSITE VULNERABILITY ASSESSMENT (AVA_COMP) 352
17.3.1 General 352
17.3.2 Evaluation of sub-activity (AVA_COMP.1) 352

18 CLASS ACO: COMPOSITION 354

18.1 GENERAL 354
18.2 APPLICATION NOTES 354
18.3 COMPOSITION RATIONALE (ACO_COR) 355
18.3.1 Evaluation of sub-activity (ACO_COR.1) 355
18.4 DEVELOPMENT EVIDENCE (ACO_DEV) 362
18.4.1 Evaluation of sub-activity (ACO_DEV.1) 362
18.4.2 Evaluation of sub-activity (ACO_DEV.2) 363

 © ISO/IEC 2022 – All rights reserved

18.4.3 Evaluation of sub-activity (ACO_DEV.3) *365*
18.5 RELIANCE OF DEPENDENT COMPONENT (ACO_REL) 368
18.5.1 Evaluation of sub-activity (ACO_REL.1) *368*
18.5.2 Evaluation of sub-activity (ACO_REL.2) *370*
18.6 COMPOSED TOE TESTING (ACO_CTT) 372
18.6.1 Evaluation of sub-activity (ACO_CTT.1) *372*
18.6.2 Evaluation of sub-activity (ACO_CTT.2) *375*
18.7 COMPOSITION VULNERABILITY ANALYSIS (ACO_VUL) 378
18.7.1 Evaluation of sub-activity (ACO_VUL.1) *378*
18.7.2 Application notes *378*
18.7.3 Evaluation of sub-activity (ACO_VUL.2) *381*
18.7.4 Evaluation of sub-activity (ACO_VUL.3) *384*

ANNEX A (INFORMATIVE) GENERAL EVALUATION GUIDANCE 389
A.1 OBJECTIVES 389
A.2 SAMPLING 389
A.3 DEPENDENCIES 391
A.3.1 GENERAL 391
A.3.2 DEPENDENCIES BETWEEN ACTIVITIES 391
A.3.3 DEPENDENCIES BETWEEN SUB-ACTIVITIES 391
A.3.4 DEPENDENCIES BETWEEN ACTIONS 391
A.4 SITE VISITS 391
A.4.1 GENERAL 391
A.4.2 GENERAL APPROACH 392
A.5 ORIENTATION GUIDE FOR THE PREPARATION OF THE CHECKLIST 393
A.5.1 ASPECTS OF CONFIGURATION MANAGEMENT 393
A.5.2 ASPECTS OF DEVELOPMENT SECURITY 393
A.5.3 EXAMPLE OF A CHECKLIST 394
A.6 SCHEME RESPONSIBILITIES 397
ANNEX B (INFORMATIVE) VULNERABILITY ASSESSMENT (AVA) 399
B.1 WHAT IS VULNERABILITY ANALYSIS 399
B.2 EVALUATOR CONSTRUCTION OF A VULNERABILITY ANALYSIS 399
B.3 GENERIC VULNERABILITY GUIDANCE 400
B.3.1 BYPASSING 400
B.3.2 TAMPERING 402
B.3.3 DIRECT ATTACKS 405
B.3.4 MONITORING 405
B.3.5 MISUSE 406
B.4 IDENTIFICATION OF POTENTIAL VULNERABILITIES 407
B.4.1 ENCOUNTERED 407
B.4.2 ANALYSIS 408
B.4.2.1 GENERAL 408
B.4.2.2 UNSTRUCTURED ANALYSIS 408

© ISO/IEC 2022 – All rights reserved

B.4.2.3 FOCUSED 408
B.4.2.4 METHODICAL 409
B.5 WHEN ATTACK POTENTIAL IS USED 410
B.5.1 DEVELOPER 410
B.5.2 EVALUATOR 410
B.6 CALCULATING ATTACK POTENTIAL 411
B.6.1 APPLICATION OF ATTACK POTENTIAL 411
B.6.1.1 GENERAL 411
B.6.1.2 TREATMENT OF MOTIVATION 411
B.6.2 CHARACTERISING ATTACK POTENTIAL 412
B.6.2.1 GENERAL 412
B.6.2.2 DETERMINING THE ATTACK POTENTIAL 412
B.6.2.3 FACTORS TO BE CONSIDERED 412
B.6.2.4 CALCULATION OF ATTACK POTENTIAL 415
B.7 EXAMPLE CALCULATION FOR DIRECT ATTACK 418
ANNEX C (INFORMATIVE) EVALUATION TECHNIQUES AND TOOLS 420
C.1 SEMIFORMAL AND FORMAL METHODS 420
C.1.1 GENERAL 420
C.1.2 DESCRIPTION OF STYLES 420
C.1.2.1 INFORMAL STYLE 421
C.1.2.2 SEMIFORMAL STYLE 422
C.1.2.3 FORMAL STYLE 423

 © ISO/IEC 2022 – All rights reserved

List of figures

FIGURE 1 — MAPPING OF THE ISO/IEC 15408 SERIES AND ISO/IEC 18045 STRUCTURES 5
FIGURE 2 — GENERIC EVALUATION MODEL 7
FIGURE 3 — EXAMPLE OF THE VERDICT ASSIGNMENT RULE 8
FIGURE 4 — ETR INFORMATION CONTENT FOR A PP EVALUATION 12
FIGURE 5 — ETR INFORMATION CONTENT FOR A PP-CONFIGURATION EVALUATION 14
FIGURE 6 — ETR INFORMATION CONTENT FOR A TOE EVALUATION 17
FIGURE 7 — RELATIONSHIP BETWEEN PPS AND PP-MODULES IN A PP-CONFIGURATION 50
FIGURE 8 — EXAMPLE OF EXACT CONFORMANCE RELATIONSHIPS BETWEEN AN ST AND PPS 94

© ISO/IEC 2022 – All rights reserved

List of tables

TABLE 1 — ASE_COMP 127
TABLE 2 — ADV_COMP 214
TABLE 3 — ALC_COMP 284
TABLE 4 — ATE_COMP 316
TABLE 5 — AVA_COMP 352
TABLE A.1 — EXAMPLE OF A CHECKLIST AT EAL 4 (EXTRACT) 395
TABLE B.1 — VULNERABILITY TESTING AND ATTACK POTENTIAL 410
TABLE B.2 — CALCULATION OF ATTACK POTENTIAL 415
TABLE B.3 — RATING OF VULNERABILITIES AND TOE RESISTANCE 417

 © ISO/IEC 2022 – 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).

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) or the IEC list of patent declarations received (see http://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. 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*.

This third edition cancels and replaces the second edition (ISO/IEC 18045:2008), which has been technically revised.

The main changes are as follows:

— the exact conformance type has been introduced;
— low assurance PPs have been removed and direct rationale PPs have been introduced;
— PP-modules and PP-configurations for modular evaluations have been introduced;
— multi-assurance evaluation has been introduced.

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 2022 – All rights reserved

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	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

 © ISO/IEC 2022 – All rights reserved

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.

NOTE 1 Reference throughout the document to ISO/IEC 15408 implies the ISO/IEC 15408 series.

NOTE 2 This document uses bold and italic type in some cases to distinguish terms from the rest of the text. The relationship between components within a family is highlighted using a bolding convention. This convention calls for the use of bold type for all new requirements. For hierarchical components, requirements are presented in bold type when they are enhanced or modified beyond the requirements of the previous component. In addition, any new or enhanced permitted operations beyond the previous component are also highlighted using bold type.

The use of italics indicates text that has a precise meaning. For security assurance requirements the convention is for special verbs relating to evaluation.

© ISO/IEC 2022 – All rights reserved

INTERNATIONAL STANDARD **ISO/IEC 18045:2022(E)**

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 15408-1:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3:2022, *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*

koniec náhľadu – text ďalej pokračuje v platenej verzii STN

© ISO/IEC 2022 – All rights reserved