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

Copyrighted - no reproduction and circulation
For CCCY's review

Reference number
ISO/IEC 18045:2022(E)

Documents
Document Sharing Hub
© ISO/IEC 2022

Full document details: ISO_IEC 18045 (WG)_2022

Copyrighted - no reproduction and circulation
For CCCY's review

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

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub

Full document details: ISO_IEC 18045 (WG)_2022

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*

Copyrighted - no reproduction and circulation
For COCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

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

Copyrighted: no reproduction and circulation
For COOY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

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*

Copyrighted - no reproduction and circulation
For CCCY's review

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: ISO_IEC 18045 (WG)_2022

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

Copyrighted material
Copyright ISO/IEC 2022 – All rights reserved
For COOY's review
Documents
Document Sharing Hub

Full document details: ISO_IEC 18045 (WG)_2022

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

Copyrighted - no reproduction and circulation
For CCCV's review

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: ISO_IEC 18045 (WG)_2022

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

Copyrighted - no reproduction and circulation
For COCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

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

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

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

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

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.

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

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

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

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.

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

Copyrighted - no reproduction and circulation
For CCCY's review

Documents
Document Sharing Hub

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*

3 Terms and definitions

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 15408-4, ISO/IEC 15408-5, ISO/IEC IEEE 24765 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- IEC Electropedia: available at https://www.electropedia.org/
- ISO Online browsing platform: available at https://www.iso.org/obp/

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.

Copyrighted - No reproduction and circulation For CCCY's review

© ISO/IEC 2022 – All rights reserved

Documents Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

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" which imply that an analysis has already been performed which needs to be reviewed.

3.6
encountered potential vulnerability
potential weakness in the target of evaluation (TOE) identified by the evaluator while performing evaluation activities that can be used to violate the security functional requirements (SFRs)

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

Copyrighted - no reproduction and circulation
For CCCV's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

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.

3.12
justify, verb
<evaluation> provide a rationale providing sufficient reason

Note 1 to entry: The term 'justify' is more rigorous than '*demonstrate*' (3.3). This term requires significant rigour in terms of very carefully and thoroughly *explaining* (3.11) every step of a logical analysis leading to a conclusion.

3.13
monitoring attack
generic category of attack methods that includes passive analysis techniques aiming at disclosure of sensitive internal data of the target of evaluation (TOE) by operating the TOE in the way that corresponds to the guidance documents

3.14
observation report
OR
report written by the evaluator requesting a clarification or identifying a problem during the evaluation

3.15
oversight verdict
statement issued by an evaluation authority confirming or rejecting an overall verdict based on the results of evaluation oversight activities

3.16
prove, verb
<evaluation> show correspondence by formal analysis in its mathematical sense

Note 1 to entry: It is completely rigorous in all ways. Typically, the term "prove" is used when there is a desire to show correspondence between two target of evaluation (TOE) security functionality (TSF) representations at a high level of rigour.

3.17
record, verb
<evaluation> 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

3.18
report, verb
<evaluation> include evaluation results and supporting material in the evaluation technical report, an *observation report* (3.14) or an evaluation authority report (report of the evaluation authority)

3.19
specify, verb
<evaluation> provide specific details about an entity in a rigorous and precise manner

Copyrighted - no reproduction and circulation
For CCCV's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

3.20
trace, verb
<evaluation> establish a relation between two sets of entities, which shows which entities in the first set correspond to which entities in the second

3.21
verdict
statement issued by an evaluator with respect to evaluator action element, assurance component, or class

3.22
verify, verb
<evaluation> rigorously review in detail with an independent determination of sufficiency

Note 1 to entry: Also see "*confirm*" (3.2). This term has more rigorous connotations. The term "verify" is used in the context of evaluator actions where an independent effort is required of the evaluator.

3.23
window of opportunity
period of time that an attacker has access to the target of evaluation (TOE)

3.24
work unit
most granular level of evaluation work

4 Abbreviated terms

OR observation report

5 Terminology

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

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

6 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 therefore only within the work units and sub-tasks. The work units and sub-tasks contain mandatory activities that the evaluator must perform in order to assign verdicts.

Guidance text accompanying work units and sub-tasks gives further explanation on how to apply ISO/IEC 15408 words in an evaluation. The verb usage is in accordance with ISO definitions for these verbs. The auxiliary verb *should* is used to indicate a recommendation. *May* indicates a permission and *can* indicates a possibility.

The verbs *check*, *examine*, *report* and *record* are used with a precise meaning within this part of this document and Clause 3 should be referenced for their definitions.

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

7 General evaluation guidance

Material that has applicability to more than one sub-activity is collected in one place. Guidance whose applicability is widespread (across activities and EALs) has been collected into Annex A. Guidance that pertains to multiple sub-activities within a single activity has been provided in the introduction to that activity. If guidance pertains to only a single sub-activity, it is presented within that sub-activity.

8 Relationship between the ISO/IEC 15408 series and ISO/IEC 18045 structures

There are direct relationships between the ISO/IEC 15408 series structure (i.e. class, family, component and element) and the structure of this document. Figure 1 illustrates the correspondence between the ISO/IEC 15408 series constructs of class, family and evaluator action elements and evaluation methodology activities, sub-activities and actions. However, several evaluation methodology work units can result from the requirements noted in the ISO/IEC 15408 series developer action and content and presentation elements.

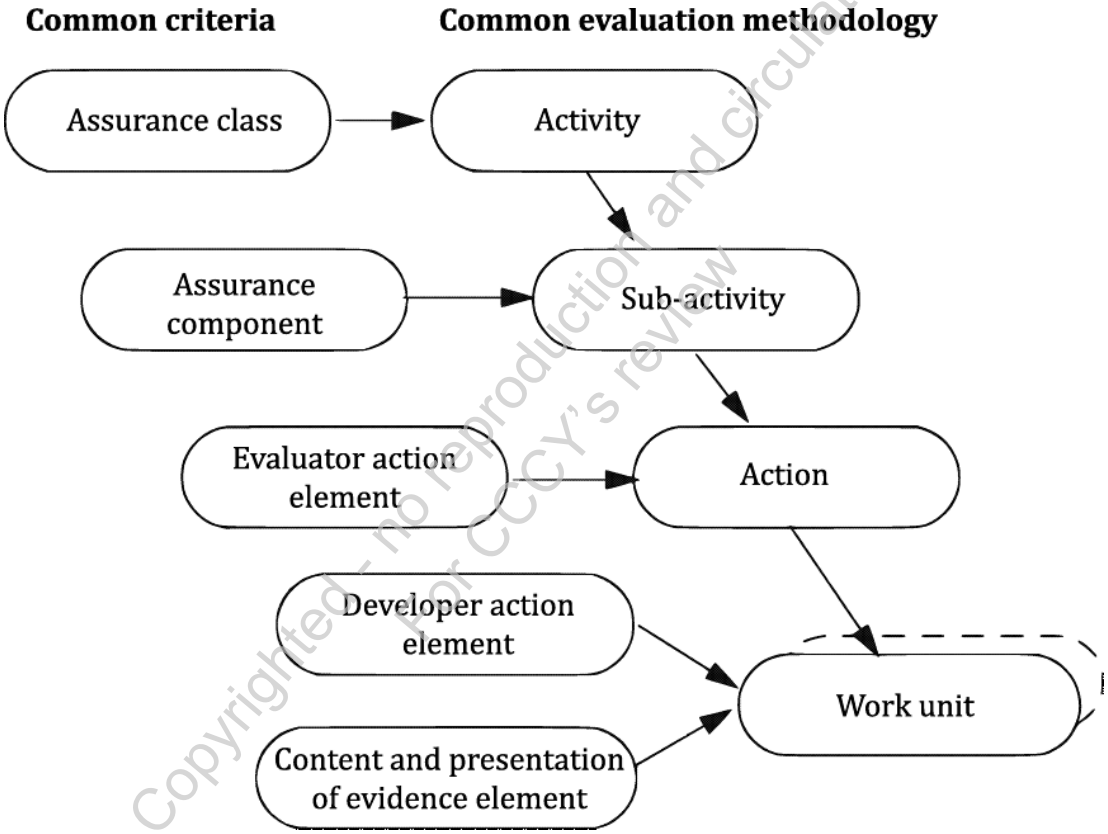

Figure 1 — Mapping of the ISO/IEC 15408 series and ISO/IEC 18045 structures

9 Evaluation process and related tasks

9.1 General

This clause provides an overview of the evaluation process and defines the tasks an evaluator is intended to perform when conducting an evaluation.

Each evaluation, whether of a PP, PP-Configuration, or TOE (including ST), follows the same process, and has four evaluator tasks in common: the input task, the output task, the evaluation sub-activities, and the demonstration of the technical competence to the evaluation authority task.

Copyrighted - no reproduction and circulation for CCCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

The input task and the output tasks, which are related to management of evaluation evidence and to report generation, are entirely described in this clause. Each task has associated sub-tasks that apply to all ISO/IEC 15408 evaluations (evaluation of a PP, PP-Configuration, or a TOE).

The evaluation sub-activities are only introduced in this clause, and fully described in the following chapters.

In contrast to the evaluation sub-activities, input and output tasks have no verdicts associated with them as they do not map to ISO/IEC 15408 evaluator action elements; they are performed in order to ensure conformance with the universal principles and to be in conformance with this document.

The demonstration of the technical competence to the evaluation authority task can be fulfilled by the evaluation authority analysis of the output tasks results, or may include the demonstration by the evaluators of their understanding of the inputs for the evaluation sub-activities. This task has no associated evaluator verdict, but has an evaluator authority verdict. The detailed criteria to pass this task are left to the discretion of the evaluation authority, as noted in A.6.

Evaluation activities defined in conformance with ISO/IEC15408-4 can be used in place of work units defined within this document provided that this is made clear within the evaluation and certification reports.

9.2 Evaluation process overview

9.2.1 Objectives

This subclause presents the general model of the methodology and identifies:

a) roles and responsibilities of the parties involved in the evaluation process;

b) the general evaluation model.

9.2.2 Responsibilities of the roles

The general model defines the following roles: sponsor, developer, evaluator and evaluation authority.

The sponsor is responsible for requesting and supporting an evaluation. This means that the sponsor establishes the different agreements for the evaluation (e.g. commissioning the evaluation). Moreover, the sponsor is responsible for ensuring that the evaluator is provided with the evaluation evidence.

The developer produces the TOE and is responsible for providing the evidence required for the evaluation (e.g. training, design information), on behalf of the sponsor.

The evaluator performs the evaluation tasks required in the context of an evaluation: the evaluator receives the evaluation evidence from the developer on behalf of the sponsor or directly from the sponsor, performs the evaluation sub-activities and provides the results of the evaluation assessment to the evaluation authority.

The evaluation authority establishes and maintains the scheme, monitors the evaluation conducted by the evaluator, and issues certification/validation reports as well as certificates based on the evaluation results provided by the evaluator.

9.2.3 Relationship of roles

To prevent undue influence from improperly affecting an evaluation, some separation of roles is required. This implies that the roles described above are fulfilled by different entities, except that the roles of developer and sponsor can be satisfied by a single entity.

Moreover, some evaluations (e.g. EAL1 evaluation) may not require the developer to be involved in the project. In this case, it is the sponsor who provides the TOE to the evaluator and who generates the evaluation evidence.

Copyrighted - no reproduction and circulation for CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

9.2.4 General evaluation model

The evaluation process consists of the evaluator performing the evaluation input task, the evaluation output task and the evaluation sub-activities. Figure 2 provides an overview of the relationship between these tasks and sub-activities.

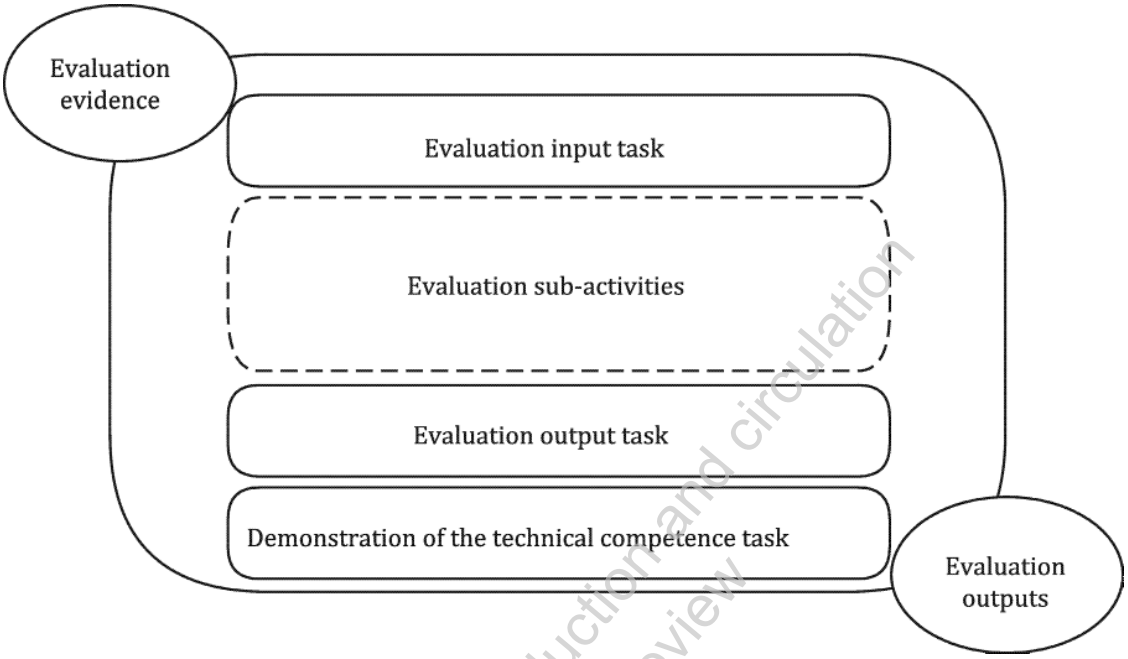

Figure 2 — Generic evaluation model

The evaluation process may be preceded by a preparation phase where initial contact is made between the sponsor and the evaluator. The work that is performed and the involvement of the different roles during this phase may vary. It is typically during this step that the evaluator performs a feasibility analysis to assess the likelihood of a successful evaluation.

9.2.5 Evaluator verdicts

The evaluator assigns verdicts to the requirements of ISO/IEC 15408 and not to those of this document. The most granular ISO/IEC 15408 structure to which a verdict is assigned is the evaluator action element (explicit or implied). A verdict is assigned to an applicable ISO/IEC 15408 evaluator action element as a result of performing the corresponding evaluation methodology action and its constituent work units. Where required by a Security Target, the evaluator may follow Evaluation Activities derived from work units in this document (for example using the framework in ISO/IEC 15408-4:2022). Where such derived Evaluation Methods and Evaluation Activities are required by an ST then these shall be used by the evaluator to assign verdicts to the relevant evaluator action element(s). Finally, an evaluation result is assigned, as described in ISO/IEC 15408-1:2022, Clause 13, Evaluation and evaluation results.

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

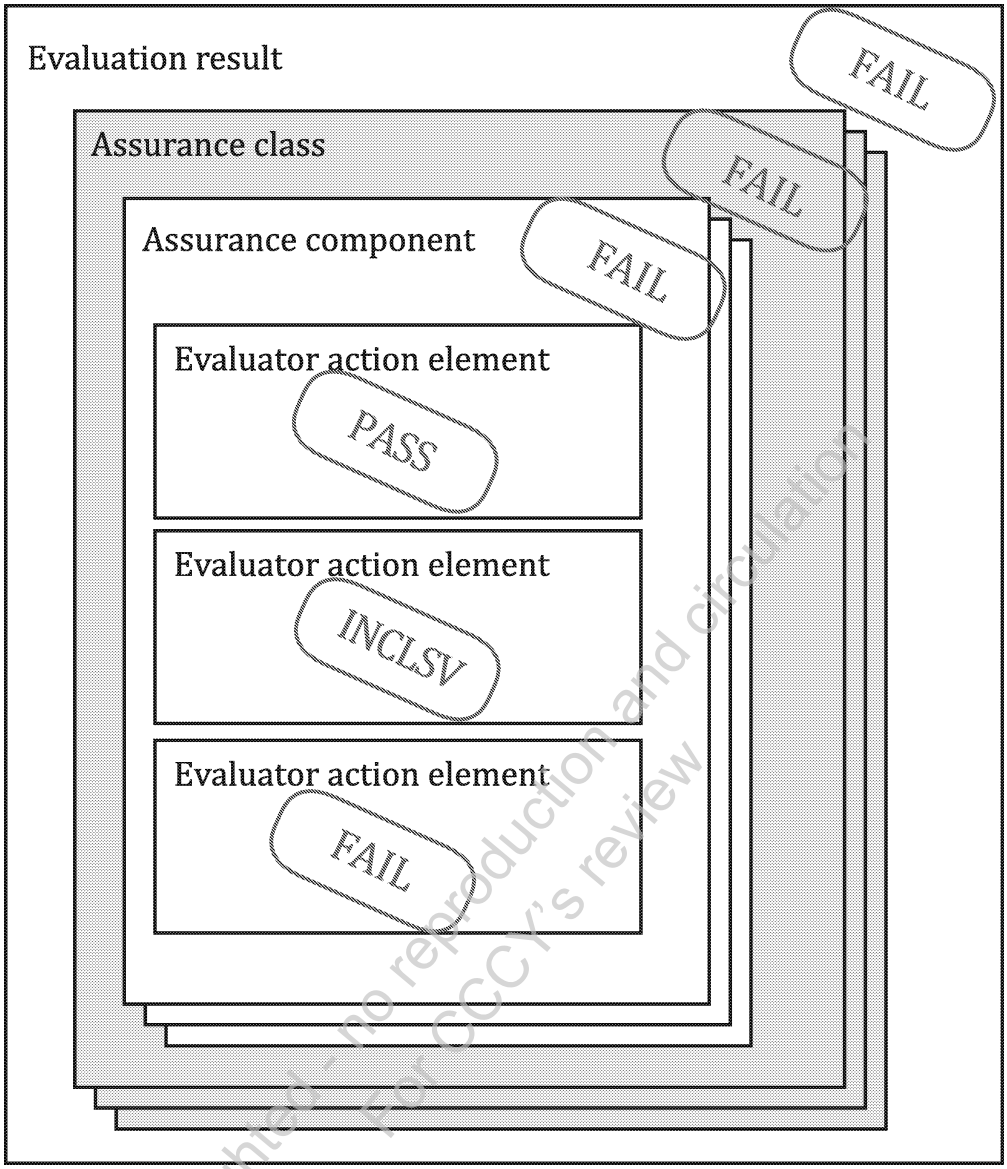

Figure 3 — Example of the verdict assignment rule

Copyrighted - no reproduction and circulation for CCCY's review

This document recognises three mutually exclusive verdict states:

a) conditions for a pass verdict are defined as an evaluator completion of ISO/IEC 15408 evaluator action element and determination that the requirements for the PP, PP-Configuration, ST or TOE under evaluation are met. The conditions for passing the element are defined as:

   1) the constituent work units of the related evaluation methodology action, and;

   2) all evaluation evidence required for performing these work units is coherent, that is it can be fully and completely understood by the evaluator, and;

   3) all evaluation evidence required for performing these work units does not have any obvious internal inconsistencies or inconsistencies with other evaluation evidence. Note that obvious means here that the evaluator discovers this inconsistency while performing the work units: the evaluator should not undertake a full consistency analysis across the entire evaluation evidence every time a work unit is performed.

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

b) conditions for a *fail* verdict are defined as an evaluator completion of ISO/IEC 15408 evaluator action element and determination that the requirements for the PP, PP-Configuration, ST, or TOE under evaluation are not met, or that the evidence is incoherent, or an obvious inconsistency in the evaluation evidence has been found;

c) all verdicts are initially *inconclusive* and remain so until either a *pass* or *fail* verdict is assigned.

The overall verdict is *pass* if and only if all the constituent verdicts are also *pass*. In the example illustrated in Figure 3, if the verdict for one evaluator action element is *fail* then the verdicts for the corresponding assurance component, assurance class, and overall verdict are also *fail*.

9.3 Evaluation input task

9.3.1 Objectives

The objective of this task is to ensure that the evaluator has available the correct version of the evaluation evidence necessary for the evaluation and that it is adequately protected. Otherwise, the technical accuracy of the evaluation cannot be assured, nor can it be assured that the evaluation is being conducted in a way to provide repeatable and reproducible results.

9.3.2 Application notes

The responsibility to provide all the required evaluation evidence lies with the sponsor. However, most of the evaluation evidence is likely to be produced and supplied by the developer, on behalf of the sponsor.

Since the assurance requirements apply to the entire TOE, all evaluation evidence pertaining to all parts of the TOE is to be made available to the evaluator. The scope and required content of such evaluation evidence is independent of the level of control that the developer has over each of the parts of the TOE. For example, if design is required, then the TOE design (ADV_TDS) requirements will apply to all subsystems that are part of the TSF. In addition, assurance requirements that call for procedures to be in place, e.g. CM capabilities (ALC_CMC) and Delivery (ALC_DEL) will also apply to the entire TOE (including any part produced by another developer).

It is recommended that the evaluator, in conjunction with the sponsor, produce an index to required evaluation evidence. This index may be a set of references to the documentation. This index should contain enough information (e.g. a brief summary of each document, or at least an explicit title, indication of the subclauses of interest) to help the evaluator to find easily the required evidence.

It is the information contained in the evaluation evidence that is required, not any particular document structure. Evaluation evidence for a sub-activity may be provided by separate documents, or a single document may satisfy several of the input requirements of a sub-activity.

The evaluator requires stable and formally-issued versions of evaluation evidence. However, draft evaluation evidence may be provided during an evaluation, for example, to help an evaluator make an early, informal assessment, but is not used as the basis for verdicts. It may be helpful for the evaluator to see draft versions of particular appropriate evaluation evidence, such as:

a) test documentation, to allow the evaluator to make an early assessment of tests and test procedures;

b) design documents, to provide the evaluator with background for understanding the TOE design;

c) source code or hardware drawings, to allow the evaluator to assess the application of the developer's standards.

Draft evaluation evidence is more likely to be encountered where the evaluation of a TOE is performed concurrently with its development. However, it may also be encountered during the evaluation of an already-developed TOE where the developer has had to perform additional work to address a problem identified by

Copyrighted - no reproduction and circulation
For CCCRS review

© ISO/IEC 2022 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

the evaluator (e.g. to correct an error in design or implementation) or to provide evaluation evidence of security that is not provided in the existing documentation (e.g. in the case of a TOE not originally developed to meet the requirements of ISO/IEC 15408).

9.3.3 Management of evaluation evidence sub-task

9.3.3.1 Configuration control

The evaluator ***shall perform*** configuration control of the evaluation evidence.

ISO/IEC 15408 implies that the evaluator is able to identify and locate each item of evaluation evidence after it has been received and is able to determine whether a specific version of a document is in the evaluator's possession.

The evaluator ***shall protect*** the evaluation evidence from alteration or loss while it is in the evaluator's possession.

9.3.3.2 Disposal

Schemes may wish to control the disposal of evaluation evidence at the conclusion of an evaluation. The disposal of the evaluation evidence should be achieved by one or more of:

a) returning the evaluation evidence;

b) archiving the evaluation evidence;

c) destroying the evaluation evidence.

9.3.3.3 Confidentiality

An evaluator may have access to sponsor and developer commercially-sensitive information (e.g. TOE design information, specialist tools), and may have access to nationally-sensitive information during the course of an evaluation. Schemes may wish to impose requirements for the evaluator to maintain the confidentiality of the evaluation evidence. The sponsor and evaluator may mutually agree to additional requirements as long as these are consistent with the scheme.

Confidentiality requirements affect many aspects of evaluation work, including the receipt, handling, storage and disposal of evaluation evidence.

9.4 Evaluation sub-activities

The evaluation sub-activities vary depending on whether it is a PP, PP-Configuration, or a TOE evaluation. Moreover, in the case of a TOE evaluation, the sub-activities depend upon the selected assurance requirements.

9.5 Evaluation output task

9.5.1 Objectives

The objective of this subclause is to describe the Observation Report (OR) and the Evaluation Technical Report (ETR). Schemes may require additional evaluator reports such as reports on individual units of work, or may require additional information to be contained in the OR and the ETR. This document does not preclude the addition of information into these reports as this International Standard specifies only the minimum information content.

Consistent reporting of evaluation results facilitates the achievement of the universal principle of repeatability and reproducibility of results. The consistency covers the type and the amount of information

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

reported in the ETR and OR. The consistency of ETR and OR among different evaluations is the responsibility of the evaluation authority.

The evaluator performs the two following sub-tasks in order to meet the requirements of this document for the information content of reports:

a) write OR sub-task (if needed in the context of the evaluation);

b) write ETR sub-task.

9.5.2 Management of evaluation outputs

The evaluator delivers the ETR to the evaluation authority, as well as any ORs as they become available. Requirements for controls on handling the ETR and ORs are established by the scheme which may include delivery to the sponsor or developer. The ETR and ORs may include sensitive or proprietary information and may need to be sanitised before they are given to the sponsor.

9.5.3 Application notes

In this edition of this document, the requirements for the provision of evaluator evidence to support re-evaluation and re-use have not been explicitly stated. Where information for re-evaluation or re-use is required by the sponsor, the scheme under which the evaluation is being performed should be consulted.

9.5.4 Write OR sub-task

ORs provide the evaluator with a mechanism to request a clarification (e.g. from the evaluation authority on the application of a requirement) or to identify a problem with an aspect of the evaluation.

In the case of a fail verdict, the evaluator ***shall provide*** an OR to reflect the evaluation result. Otherwise, the evaluator may use ORs as one way of expressing clarification needs.

For each OR, the evaluator ***shall report*** the following:

a) the identifier of the PP or TOE evaluated;

b) the evaluation task/sub-activity during which the observation was generated;

c) the observation;

d) the assessment of its severity (e.g. implies a fail verdict, holds up progress on the evaluation, requires a resolution prior to evaluation being completed);

e) the identification of the organisation responsible for resolving the issue;

f) the recommended timetable for resolution;

g) the assessment of the impact on the evaluation of failure to resolve the observation.

The intended audience of an OR and procedures for handling the report depend on the nature of the report's content and on the scheme. Schemes may distinguish different types of ORs or define additional types, with associated differences in required information and distribution (e.g. evaluation ORs to evaluation authorities and sponsors).

9.5.5 Write ETR sub-task

9.5.5.1 Objectives

The evaluator ***shall provide*** an ETR to present technical justification of the verdicts.

Copyrighted - no reproduction and circulation
For CCCV's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

This document defines the ETR's minimum content requirement; however, schemes may specify additional content and specific presentational and structural requirements. For instance, schemes may require that certain introductory material (e.g. disclaimers and copyright clauses) be reported in the ETR.

The reader of the ETR is assumed to be familiar with general concepts of information security, ISO/IEC 15408, this document, evaluation approaches and IT.

The ETR supports the evaluation authority to confirm that the evaluation was done to the required standard, but it is anticipated that the documented results may not provide all of the necessary information, so additional information specifically requested by the scheme may be necessary. This aspect is outside the scope of this document.

9.5.5.2 ETR for a PP Evaluation

9.5.5.2.1 General

This subclause describes the minimum content of the ETR for a PP evaluation. The contents of the ETR are portrayed in Figure 4; this figure may be used as a guide when constructing the structural outline of the ETR document.

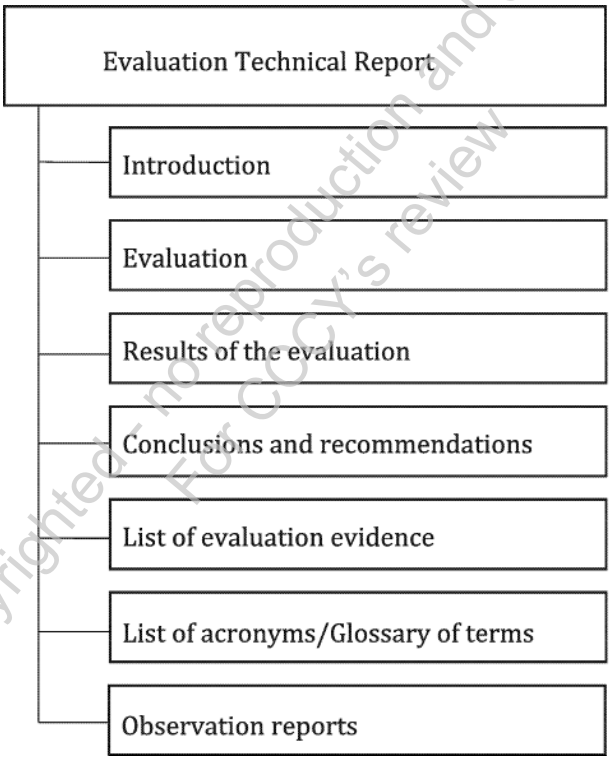

Figure 4 — ETR information content for a PP evaluation

9.5.5.2.2 General

The evaluator ***shall report*** evaluation scheme identifiers.

Evaluation scheme identifiers (e.g. logos) are the information required to unambiguously identify the scheme responsible for the evaluation oversight.

The evaluator ***shall report*** ETR configuration control identifiers.

The ETR configuration control identifiers contain information that identifies the ETR (e.g. name, date and version number).

Copyrighted - no reproduction and circulation
For COCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

The evaluator ***shall report*** PP configuration control identifiers.

PP configuration control identifiers (e.g. name, date and version number) are required to identify what is being evaluated in order for the evaluation authority to verify that the verdicts have been assigned correctly by the evaluator.

The evaluator ***shall report*** the identity of the developer.

The identity of the PP developer is required to identify the party responsible for producing the PP.

The evaluator ***shall report*** the identity of the sponsor.

The identity of the sponsor is required to identify the party responsible for providing evaluation evidence to the evaluator.

The evaluator ***shall report*** the identity of the evaluator.

The identity of the evaluator is required to identify the party performing the evaluation and responsible for the evaluation verdicts.

9.5.5.2.3 Evaluation

The evaluator ***shall report*** the evaluation methods, techniques, tools and standards used.

The evaluator references the evaluation criteria, methodology and interpretations used to evaluate the PP.

The evaluator ***shall report*** any constraints on the evaluation, constraints on the handling of evaluation results and assumptions made during the evaluation that have an impact on the evaluation results.

The evaluator may include information in relation to legal or statutory aspects, organisation, confidentiality.

9.5.5.2.4 Results of the evaluation

The evaluator ***shall report*** a verdict and a supporting rationale for each assurance component that constitutes an APE activity, as a result of performing the corresponding evaluation methodology action and its constituent work units.

The rationale justifies the verdict using ISO/IEC 15408, this document, any interpretations and the evaluation evidence examined and shows how the evaluation evidence does or does not meet each aspect of the criteria. It contains a description of the work performed, the method used, and any derivation of results. The rationale may provide detail to the level of an evaluation methodology work unit.

9.5.5.2.5 Conclusions and recommendations

The evaluator ***shall report*** the conclusions of the evaluation, in particular the overall verdict as defined in ISO/IEC 15408-1:2022, Clause 12, Evaluation results, and determined by application of the verdict assignment described in 8.2.5.

The evaluator provides recommendations that may be useful for the evaluation authority. These recommendations may include shortcomings of the PP discovered during the evaluation or mention of features which are particularly useful.

9.5.5.2.6 List of evaluation evidence

The evaluator ***shall report*** for each item of evaluation evidence the following information:

a) the issuing body (e.g. the developer, the sponsor);

b) the title;

Copyrighted - no reproduction and circulation
For CCCYS review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

c) the unique reference (e.g. issue date and version number).

9.5.5.2.7 List of acronyms/Glossary of terms

The evaluator ***shall report*** any acronyms or abbreviations used in the ETR.

Glossary definitions already defined by ISO/IEC 15408(all parts) or by this document need not be repeated in the ETR.

9.5.5.2.8 Observation reports

The evaluator ***shall report*** a complete list that uniquely identifies the ORs raised during the evaluation and their status.

For each OR, the list should contain its identifier as well as its title or a brief summary of its content.

9.5.5.3 ETR for a PP-Configuration Evaluation

9.5.5.3.1 General

This subclause describes the minimum content of the ETR for a PP-Configuration evaluation. The contents of the ETR are portrayed in Figure 5; this figure may be used as a guide when constructing the structural outline of the ETR document.

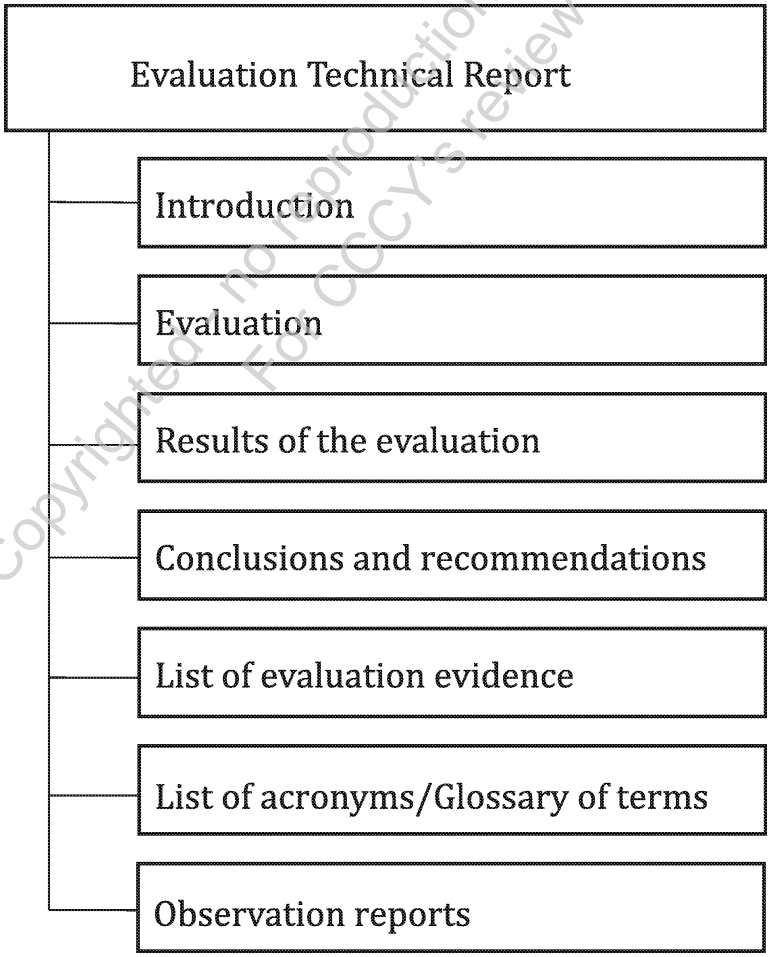

Figure 5 — ETR information content for a PP-Configuration evaluation

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

9.5.5.3.2 General

The evaluator ***shall report*** evaluation scheme identifiers.

Evaluation scheme identifiers (e.g. logos) are the information required to unambiguously identify the scheme responsible for the evaluation oversight.

The evaluator ***shall report*** ETR configuration control identifiers.

The ETR configuration control identifiers contain information that identifies the ETR (e.g. name, date and version number).

The evaluator ***shall report*** PP-Configuration configuration control identifiers.

PP configuration control identifiers (e.g. name, date and version number) are required to identify what is being evaluated in order for the evaluation authority to verify that the verdicts have been assigned correctly by the evaluator.

The evaluator ***shall report*** the identity of the developer.

The identity of the PP-Configuration developer is required to identify the party responsible for producing the PP-Configuration.

The evaluator ***shall report*** the identity of the sponsor.

The identity of the sponsor is required to identify the party responsible for providing evaluation evidence to the evaluator.

The evaluator ***shall report*** the identity of the evaluator.

The identity of the evaluator is required to identify the party performing the evaluation and responsible for the evaluation verdicts.

9.5.5.3.3 PP-Configuration overview

The evaluator ***shall report*** all PP-Configuration components used in the PP-configuration.

PP-Configuration components include at least one PP, as well as all other PPs and PP-Modules used in the PP-Configuration. Each PP-Module will have one of its PP-Module Bases included in the PP-Configuration, therefore all elements of the relevant PP-Module Base are included as PP-Configuration components. See ISO/IEC 15408-1:2022, Annex C for more detail on the identification of the PP-Module Base for each PP-Module.

The ETR **shall report** the reference of the PP-Configuration components.

A PP-Configuration component reference contains information that uniquely identifies the specific component (e.g. title, date, and version number).

9.5.5.3.4 Evaluation

The evaluator ***shall report*** the evaluation methods, techniques, tools and standards used.

The evaluator references the evaluation criteria, methodology and interpretations used to evaluate the PP-Configuration.

The evaluator ***shall report*** any constraints on the evaluation, constraints on the handling of evaluation results and assumptions made during the evaluation that have an impact on the evaluation results.

The evaluator may include information in relation to legal or statutory aspects, organisation, confidentiality.

Copyrighted - no reproduction and circulation
For CCCV's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

9.5.5.3.5 Results of the evaluation

The evaluator ***shall report*** a verdict and a supporting rationale for each assurance component that constitutes an ACE activity, as a result of performing the corresponding evaluation methodology action and its constituent work units.

The rationale justifies the verdict using ISO/IEC 15408, this document, any interpretations and the evaluation evidence examined and shows how the evaluation evidence does or does not meet each aspect of the criteria. It contains a description of the work performed, the method used, and any derivation of results. The rationale may provide detail to the level of an evaluation methodology work unit.

9.5.5.3.6 Conclusions and recommendations

The evaluator ***shall report*** the conclusions of the evaluation, in particular the overall verdict as defined in ISO/IEC 15408-1:2022, Clause 12, Evaluation results, and determined by application of the verdict assignment described in 8.2.5 .

The evaluator provides recommendations that may be useful for the evaluation authority. These recommendations may include shortcomings of the PP-Configuration discovered during the evaluation or mention of features which are particularly useful.

9.5.5.3.7 List of evaluation evidence

The evaluator ***shall report*** for each item of evaluation evidence the following information:

a) the issuing body (e.g. the developer, the sponsor);

b) the title;

c) the unique reference (e.g. issue date and version number).

9.5.5.3.8 List of acronyms/Glossary of terms

The evaluator ***shall report*** any acronyms or abbreviations used in the ETR.

Glossary definitions already defined by ISO/IEC 15408 or by this document need not be repeated in the ETR.

9.5.5.3.9 Observation reports

The evaluator ***shall report*** a complete list that uniquely identifies the ORs raised during the evaluation and their status.

For each OR, the list should contain its identifier as well as its title or a brief summary of its content.

9.5.5.4 ETR for a TOE Evaluation

9.5.5.4.1 General

This subclause describes the minimum content of the ETR for a TOE evaluation. The contents of the ETR are portrayed in Figure 6; this figure may be used as a guide when constructing the structural outline of the ETR document.

Copyrighted - no reproduction and circulation
For CCCV's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

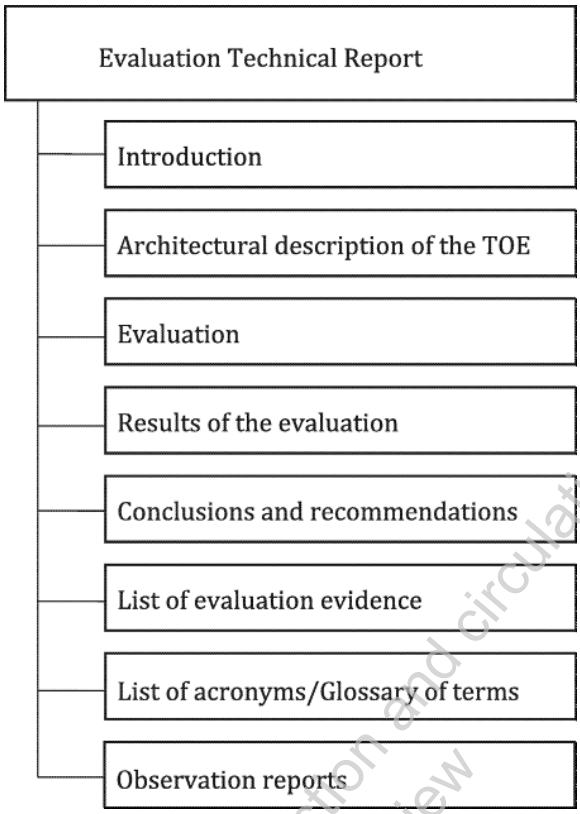

Figure 6 — ETR information content for a TOE evaluation

Copyrighted - no reproduction and circulation
For CCCY's review

9.5.5.4.2 General

The evaluator ***shall report*** evaluation scheme identifiers.

Evaluation scheme identifiers (e.g. logos) are the information required to unambiguously identify the scheme responsible for the evaluation oversight.

The evaluator ***shall report*** ETR configuration control identifiers.

The ETR configuration control identifiers contain information that identifies the ETR (e.g. name, date and version number).

The evaluator ***shall report*** ST and TOE configuration control identifiers.

ST and TOE configuration control identifiers identify what is being evaluated in order for the evaluation authority to verify that the verdicts have been assigned correctly by the evaluator.

If the ST claims that the TOE conforms to the requirements of one or more PPs, or to a PP-Configuration, the ETR shall report the reference of the corresponding PPs/PP-Configuration.

The PPs/PP-Configuration reference contains information that uniquely identifies the PPs/PP-Configuration (e.g. title, date, and version number).

The evaluator ***shall report*** the identity of the developer.

The identity of the TOE developer is required to identify the party responsible for producing the TOE.

The evaluator ***shall report*** the identity of the sponsor.

The identity of the sponsor is required to identify the party responsible for providing evaluation evidence to the evaluator.

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

The evaluator ***shall report*** the identity of the evaluator.

The identity of the evaluator is required to identify the party performing the evaluation and responsible for the evaluation verdicts.

9.5.5.4.3 Architectural description of the TOE

The evaluator ***shall report*** a high level description of the TOE and its major components based on the evaluation evidence described in ISO/IEC 15408 assurance family entitled TOE design (ADV_TDS), where applicable.

The intent of this subclause is to characterise the degree of architectural separation of the major components. If there is no TOE design (ADV_TDS) requirement in the ST, this is not applicable and is considered to be satisfied.

9.5.5.4.4 Evaluation

The evaluator ***shall report*** the evaluation methods, techniques, tools and standards used.

The evaluator may reference the evaluation criteria, methodology and interpretations used to evaluate the TOE or the devices used to perform the tests. This shall include identification of any derived Evaluation Methods and Evaluation Activities used, and a confirmation that these are as required by the Security Target (cf. ASE_CCL).

The evaluator ***shall report*** any constraints on the evaluation, constraints on the distribution of evaluation results and assumptions made during the evaluation that have an impact on the evaluation results.

The evaluator may include information in relation to legal or statutory aspects, organisation, confidentiality.

9.5.5.4.5 Results of the evaluation

For each activity on which the TOE is evaluated, the evaluator ***shall report***:

a) the title of the activity considered;

b) a verdict and a supporting rationale for each assurance component that constitutes this activity, as a result of performing the corresponding evaluation methodology action and its constituent work units.

The rationale justifies the verdict using ISO/IEC 15408, this document, any derived Evaluation Methods and Evaluation Activities required by the ST, any interpretations and the evaluation evidence examined and shows how the evaluation evidence does or does not meet each aspect of the criteria. It contains a description of the work performed, the method used, and any derivation of results. The rationale may provide detail to the level of an evaluation methodology work unit.

The evaluator ***shall report*** all information specifically required by a work unit.

For the AVA and ATE activities, work units that identify information to be reported in the ETR have been defined.

9.5.5.4.6 Conclusions and recommendations

The evaluator ***shall report*** the conclusions of the evaluation, which will relate to whether the TOE has satisfied its associated ST, in particular the overall verdict as defined in ISO/IEC 15408-1:2022, Evaluation and evaluation results, and determined by application of the verdict assignment described in 8.2.5.

The evaluator provides recommendations that may be useful for the evaluation authority. These recommendations may include shortcomings of the IT product discovered during the evaluation or mention of features which are particularly useful.

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

9.5.5.4.7 List of evaluation evidence

The evaluator ***shall report*** for each item of evaluation evidence the following information:

a) the issuing body (e.g. the developer, the sponsor);

b) the title;

c) the unique reference (e.g. issue date and version number).

9.5.5.4.8 List of acronyms/Glossary of terms

The evaluator ***shall report*** any acronyms or abbreviations used in the ETR.

Glossary definitions already defined by ISO/IEC 15408 or by this document need not be repeated in the ETR.

9.5.5.4.9 Observation reports

The evaluator ***shall report*** a complete list that uniquely identifies the ORs raised during the evaluation and their status.

For each OR, the list should contain its identifier as well as its title or a brief summary of its content.

10 Class APE: Protection Profile evaluation

10.1 General

This clause describes the evaluation of a PP. The requirements and methodology for PP evaluation are identical for each PP evaluation, regardless of the EAL (or other set of assurance requirements) that is claimed in the PP. The evaluation methodology in this clause is based on the requirements on the PP as specified in ISO/IEC 15408-3:2022 class APE.

This clause should be used in conjunction with ISO/IEC 15408-1:2022, Annexes B and D, as these Annexes clarify the concepts here and provide many examples.

10.2 Re-using the evaluation results of certified PPs

While evaluating a PP that is based on one or more certified PPs, it may be possible to re-use the fact that these PPs were certified. The potential for re-use of the result of a certified PP is greater if the PP under evaluation does not add threats, OSPs, security objectives and/or security requirements to those of the PP that conformance is being claimed to. If the PP under evaluation contains much more than the certified PP, re-use may not be useful at all.

The evaluator is allowed to re-use the PP evaluation results by doing certain analyses only partially or not at all if these analyses or parts thereof were already done as part of the PP evaluation. While doing this, the evaluator should assume that the analyses in the PP were performed correctly.

An example would be where the PP that conformance is being claimed to contains a set of security requirements, and these were determined to be internally consistent during its evaluation. If the PP under evaluation uses the exact same requirements, the consistency analysis does not have to be repeated during the PP evaluation. If the PP under evaluation adds one or more requirements, or performs operations on these requirements, the analysis will have to be repeated. However, it may be possible to save work in this consistency analysis by using the fact that the original requirements are internally consistent. If the original requirements are internally consistent, the evaluator only has to determine that:

a) the set of all new and/or changed requirements is internally consistent, and

b) the set of all new and/or changed requirements is consistent with the original requirements.

Copyrighted - no reproduction and circulation
For CCCVS review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

The evaluator notes in the ETR each case where analyses are not done or only partially done for this reason.

10.3 PP introduction (APE_INT)

10.3.1 Evaluation of sub-activity (APE_INT.1)

10.3.1.1 Objectives

The objective of this sub-activity is to determine whether the PP is correctly identified, and whether the PP reference and TOE overview are consistent with each other.

10.3.1.2 Input

The evaluation evidence for this sub-activity is:

a) the PP.

10.3.1.3 Action APE_INT.1.1E

10.3.1.3.1 General

ISO/IEC 15408-3:2022 APE_INT.1.1C: *The PP introduction shall contain a PP reference and a TOE overview.*

10.3.1.3.2 Work unit APE_INT.1-1

The evaluator ***shall check*** that the PP introduction contains a PP reference and a TOE overview.

ISO/IEC 15408-3:2022 APE_INT.1.2C: *The PP reference shall uniquely identify the PP.*

10.3.1.3.3 Work unit APE_INT.1-2

The evaluator ***shall examine*** the PP reference to determine that it uniquely identifies the PP.

The evaluator determines that the PP reference identifies the PP itself, so that it may be easily distinguished from other PPs, and that it also uniquely identifies each version of the PP, e.g. by including a version number and/or a date of publication.

The PP should have some referencing system that is capable of supporting unique references (e.g. use of numbers, letters or dates).

ISO/IEC 15408-3:2022 APE_INT.1.3C: *The TOE overview shall summarize the usage and major security features of the TOE.*

10.3.1.3.4 Work unit APE_INT.1-3

The evaluator ***shall examine*** the TOE overview to determine that it describes the usage and major security features of the TOE.

The TOE overview should briefly (i.e. several paragraphs) describe the usage and major security features expected of the TOE. The TOE overview should enable consumers and potential TOE developers to quickly determine whether the PP is of interest to them.

The evaluator determines that the overview is clear enough for TOE developers and consumers, and sufficient to give them a general understanding of the intended usage and major security features of the TOE.

ISO/IEC 15408-3:2022 APE_INT.1.4C: *The TOE overview shall identify the TOE type.*

10.3.1.3.5 Work unit APE_INT.1-4

The evaluator ***shall check*** that the TOE overview identifies the TOE type.

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

ISO/IEC 15408-3:2022 APE_INT.1.5C: *The TOE overview shall identify any non-TOE hardware/software/firmware available to the TOE.*

10.3.1.3.6 Work unit APE_INT.1-5

The evaluator ***shall examine*** the TOE overview to determine that it identifies any non-TOE hardware/software/firmware available to the TOE.

While some TOEs may run stand-alone, other TOEs (notably software TOEs) need additional hardware, software or firmware to operate. In this subclause of the PP, the PP author lists all hardware, software, and/or firmware that will be available for the TOE to run on.

This identification should be detailed enough for potential consumers and TOE developers to determine whether their TOE may operate with the listed hardware, software and firmware.

10.4 Conformance claims (APE_CCL)

10.4.1 Evaluation of sub-activity (APE_CCL.1)

10.4.1.1 Objectives

The objective of this sub-activity is to determine the validity of various conformance claims. These describe how the PP conforms to ISO/IEC 15408, other PPs and packages.

10.4.1.2 Input

The evaluation evidence for this sub-activity is:

a) the PP;

b) the package(s) that the PP claims conformance to.

10.4.1.3 Action APE_CCL.1.1E

10.4.1.3.1 General

ISO/IEC 15408-3:2022 APE_CCL.1.1C: *The conformance claim shall identify the ISO/IEC 15408 edition to which the PP claims conformance.*

10.4.1.3.2 Work unit APE_CCL.1-1

The evaluator ***shall check*** that the conformance claim identifies the edition of ISO/IEC 15408 to which the PP claims conformance.

The evaluator determines that ISO/IEC 15408 conformance claim identifies the edition of ISO/IEC 15408 that was used to develop this PP. This should include the edition number of ISO/IEC 15408 and, unless the International English edition of ISO/IEC 15408 was used, the language of the edition of ISO/IEC 15408 that was used.

ISO/IEC 15408-3:2022 APE_CCL.1.2C: *The conformance claim shall describe the conformance of the PP to ISO/IEC 15408-2 as either ISO/IEC 15408-2 conformant or ISO/IEC 15408-2 extended.*

10.4.1.3.3 Work unit APE_CCL.1-2

The evaluator ***shall check*** that ISO/IEC 15408 conformance claim states a claim of either ISO/IEC 15408-2 conformant or ISO/IEC 15408-2 extended for the PP.

ISO/IEC 15408-3:2022 APE_CCL.1.3C: *The conformance claim shall describe the conformance of the PP as either "ISO/IEC 15408-3 conformant" or "ISO/IEC 15408-3:2022 extended".*

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

10.4.1.3.4 Work unit APE_CCL.1-3

The evaluator ***shall check*** that ISO/IEC 15408 conformance claim states a claim of either ISO/IEC 15408-3:2022 conformant or ISO/IEC 15408-3:2022 extended for the PP.

ISO/IEC 15408-3:2022 APE_CCL.1.4C: *The conformance claim shall be consistent with the extended components definition.*

10.4.1.3.5 Work unit APE_CCL.1-4

The evaluator ***shall examine*** the ISO/IEC 15408 conformance claim for ISO/IEC 15408-2 to determine that it is consistent with the extended components definition.

If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-2 conformant, the evaluator determines that the extended components definition does not define functional components.

If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-2 extended, the evaluator determines that the extended components definition defines at least one extended functional component.

10.4.1.3.6 Work unit APE_CCL.1-5

The evaluator ***shall examine*** the ISO/IEC 15408 conformance claim for ISO/IEC 15408-3:2022 to determine that it is consistent with the extended components definition.

If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-3:2022 conformant, the evaluator determines that the extended components definition does not define assurance components.

If ISO/IEC 15408 conformance claim contains ISO/IEC 15408-3:2022 extended, the evaluator determines that the extended components definition defines at least one extended assurance component.

ISO/IEC 15408-3:2022 APE_CCL.1.5C: *The conformance claim shall identify all PPs and packages to which the PP claims conformance.*

10.4.1.3.7 Work unit APE_CCL.1-6

The evaluator ***shall check*** that the conformance claim contains a PP claim that identifies all PPs for which the PP claims conformance.

If the PP does not claim conformance to another PP, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that any referenced PPs are unambiguously identified (e.g. by title and version number, or by the identification included in the introduction of that PP).

The evaluator is reminded that claims of partial conformance to a PP are not permitted.

If the PP is of exact conformance type, the evaluator determines that the PP claims conformance to no other PPs. If the PP is not of exact conformance type, the evaluator determines that any PPs to which conformance is claimed do not require exact conformance in their conformance statement.

10.4.1.3.8 Work unit APE_CCL.1-7

The evaluator ***shall check***, for each identified functional package, that the package definition is complete.

If the PP does not claim conformance to a functional package, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that the package definition is conformant to the requirements from ISO/IEC 15408-1:2022, Clause 9 "Packages" by checking that the functional package includes:

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

a) A functional package identification, giving a unique name, version, date, sponsor, and the ISO/IEC 15408 edition;

b) A functional package overview, giving a narrative description of the security functionality;

c) A component rationale that provides the rationale for selecting the functional components/requirements included in the package;

d) If the package defines an SPD then:

   i. the package includes a security requirements rationale.

   ii. the package includes a security objectives rationale if security objectives for the environment are defined.

   iii. If the package is a direct rationale package, there are no security objectives for the TOE defined and the security requirements rationale maps directly to the SPD.

   iv. If the package is not a direct rationale package, then security objectives for the TOE are defined, the security objectives rationale covers the objectives with respect to the SPD, and the security requirements rationale maps the requirements to the security objectives.

e) one or more security components or requirements (the functional package SFRs);

f) If extended components have been specified then the functional package includes an extended components definition;

10.4.1.3.9 Work unit APE_CCL.1-8

The evaluator ***shall check***, for each identified assurance package, that the package definition is complete. If the PP does not claim conformance to an assurance package, this work unit is not applicable and therefore considered to be satisfied. If the assurance package is a reference to one of the assurance packages contained in ISO/IEC 15408-5:2022 then this work unit is also considered to be satisfied. The evaluator determines that the package definition is conformant to the requirements from ISO/IEC 15408-1:2022, Clause 9 "Packages" by checking that the assurance package includes:

a) An assurance package identification, giving a unique name, version, date, sponsor, and the ISO/IEC 15408 edition;

b) An assurance package overview, giving a narrative description of the security functionality;

c) One or more security components or requirements (the assurance package SARs) drawn from ISO/IEC 15408-3, extended assurance components or some combination of both;

d) An assurance package shall not include an SPD or security objectives;

e) If extended components have been specified then the assurance package includes an extended components definition;

f) A security requirements rationale that provides the rationale for selecting the assurance components/ requirements included in the package.

ISO/IEC 15408-3:2022 APE_CCL.1.6C: *The conformance claim shall describe any conformance of the PP to a functional package as one of package-conformant, package-augmented, or package-tailored.*

Copyrighted - no reproduction and circulation
For CCC's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

10.4.1.3.10 Work unit APE_CCL.1-9

The evaluator ***shall check*** that, for each identified functional package, the conformance claim states a claim of conformance to that package as one of package-conformant, package-augmented, or package-tailored. If the PP does not claim conformance to a functional package, this work unit is not applicable and therefore considered to be satisfied.

If the package conformance claim contains package-conformant, the evaluator determines that all assumptions, threats, OSPs, security objectives and SFRs included in the package are included in identical form in the PP (after allowing for iteration, refinement, assignments and selections from the package to be completed as required by the PP).

If the package conformance claim contains package-augmented, the evaluator determines that all assumptions, threats, OPSs, Security Objectives, and SFRs included in the package are included in identical form in the PP (after allowing for iteration, refinement, assignments and selections from the package to be completed as required by the PP) except that the PP shall have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the functional package.

If the package conformance claim contains package-tailored, the evaluator determines that all assumptions, threats, OPSs, Security Objectives, and SFRs included in the package are included in identical form in the PP (after allowing for iteration, refinement, assignments and selections from the package to be completed as required by the PP) except that the PP shall include additional selection values for at least one of the SFRs in the package, and may also have one or more SFRs that are hierarchically higher than an SFR in the functional package.

ISO/IEC 15408-3:2022 APE_CCL.1.7C: *The conformance claim shall describe any conformance of the PP to an assurance package as either package-conformant or package-augmented.*

10.4.1.3.11 Work unit APE_CCL.1-10

The evaluator ***shall check*** that, for each identified assurance package, the conformance claim states a claim of conformance to that package as one of package-conformant or package-augmented.

If the package conformance claim contains package-conformant, the evaluator determines that the PP contains all SARs included in the package, but no additional SARs.

If the package conformance claim contains package-augmented, the evaluator determines that the PP contains all SARs included in the package, and at least one additional SAR or at least one SAR that is hierarchical to a SAR in the package.

ISO/IEC 15408-3:2022 APE_CCL.1.8C: *The conformance claim shall describe any conformance of the PP to another PP as PP Conformant.*

10.4.1.3.12 Work unit APE_CCL.1-11

The evaluator ***shall check*** that if the PP claims conformance to another PP, that claim is described as PP Conformant.

If the PP does not claim conformance to another PP, this work unit is considered satisfied.

ISO/IEC 15408-3:2022 APE_CCL.1.9C: *The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PP(s) to which conformance is being claimed.*

10.4.1.3.13 Work unit APE_CCL.1-12

The evaluator ***shall examine*** the conformance claim rationale to determine that the TOE type of the TOE is consistent with all TOE types of the PPs.

Copyrighted - No reproduction and circulation For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

If the PP does not claim conformance to another PP, this work unit is not applicable and therefore considered to be satisfied.

The relation between the types may be simple: a firewall PP claiming conformance to another firewall PP, or more complex: a smart card PP claiming conformance to a number of other PPs at the same time: a PP for the integrated circuit, a PP for the smart card OS, and two PPs for two applications on the smart card.

ISO/IEC 15408-3:2022 APE_CCL.1.10C: *The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs and any functional packages for which conformance is being claimed.*

10.4.1.3.14 Work unit APE_CCL.1-13

The evaluator ***shall examine*** the conformance claim rationale to determine that it demonstrates that the statement of security problem definition is consistent with the statements of security problem definition stated in the PPs and functional packages to which conformance is being claimed, taking into consideration the conformance statement of PPs to which conformance is being claimed.

If the PP under evaluation does not claim conformance with any PP or functional packages, this work unit is not applicable and therefore considered to be satisfied.

If the conformance claim includes functional packages, the evaluator determines that the security problem definition of the PP under evaluation consists of all assumptions, threats and OSPs of all functional packages.

The terms exact, strict and demonstrable conformance are defined in ISO/IEC 15408-1.

If packages are used, the rules defined in the following paragraphs concerning strict and demonstrable conformance also hold for the SPD descriptions taken from the packages.

Note that since a PP that specifies strict or demonstrable conformance in its conformance statement can only claim conformance to another PP whose conformance statement requires strict or demonstrable conformance, those are the only cases covered in the following paragraphs. If strict conformance is required by the PP to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator determines whether:

a) the threats in the PP under evaluation are a superset of or identical to the threats in the PP to which conformance is being claimed;

b) the OSPs in the PP under evaluation are a superset of or identical to the OSPs in the PP to which conformance is being claimed;

c) the assumptions in the PP claiming conformance are identical to the assumptions in the PP to which conformance is being claimed, with two possible exceptions described in the following two bullet points:

- an assumption (or part of an assumption) from the PP to which conformance is claimed, can be omitted, if all security objectives for the operational environment addressing this assumption (or part of an assumption) are replaced by security objectives for the TOE;

- an assumption can be added to the assumptions defined in the PP to which conformance is claimed, if a justification is given, why the new assumption neither mitigates a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the PP to which conformance is claimed, nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the PP to which conformance is claimed.

The following discussion gives some motivation and examples for cases where a PP, omits assumptions from another PP to which conformance is claimed, or adds new assumptions:

Copyrighted - no reproduction and circulation
For CCDB's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

- example for omitting an assumption: A PP to which conformance is claimed, may contain an assumption stating that the operational environment prevents unauthorized modification or interception of data sent to an external interface of the TOE. This may be the case if the TOE accepts data in clear text and without integrity protection at this interface and is assumed to be located in a secure operational environment, which will prevent attackers from accessing these data. The assumption will then be mapped in the PP, to which conformance is claimed, to some objective for the operational environment stating that the data interchanged at this interface are protected by adequate measures in the operational environment. If a PP claiming this PP, defines a more secure TOE, which has an additional security objective stating that the TOE itself protects these data, for example by providing a secure channel for encryption and integrity protection of all data transferred via this interface, the corresponding objective and assumption for the operational environment can be omitted from the PP claiming conformance. This is also called re-assigning of the objective, since the objective is re-assigned from the operational environment to the TOE. Note, that this TOE is still secure in an operational environment fulfilling the omitted assumption and therefore still fulfils the PP to which conformance is claimed.

- example for adding an assumption: In this example, the PP to which conformance is claimed, is designed to specify requirements for a TOE of type "Firewall" and the author of another PP wishes to claim conformance to this PP for a TOE, which implements a firewall, but additionally provides the functionality of a virtual private network (VPN) component. For the VPN functionality, the TOE needs cryptographic keys and these keys may also have to be handled securely by the operational environment (e. g. if symmetric keys are used to secure the network connection and therefore need to be provided in some secure way to other components in the network). In this case, it is acceptable to add an assumption that the cryptographic keys used by the VPN are handled securely by the operational environment. This assumption does not address threats or OSPs of the PP to which conformance is claimed, and therefore fulfils the conditions stated above.

- counterexample for adding an assumption: In a variant of the first example a PP to which conformance is claimed, may already contain an objective for the TOE to provide a secure channel for one of its interfaces, and this objective is mapped to a threat of unauthorized modification or reading of the data on this interface. In this case, it is clearly not allowed for another PP claiming this PP, to add an assumption for the operational environment, which assumes that the operational environment protects data on this interface against modification or unauthorized reading of the data. This assumption would reduce a threat, which is meant to be addressed by the TOE. Therefore, a TOE fulfilling a PP with this added assumption would not automatically fulfil the PP to which conformance is claimed, anymore and this addition is therefore not allowed.

- second counterexample for adding an assumption: In the example above of a TOE implementing a firewall it would not be admissible to add a general assumption that the TOE is only connected to trusted devices, because this would obviously remove essential threats relevant for a firewall (namely that there is untrusted IP traffic, which needs to be filtered). Therefore, this addition would not be allowed.

If demonstrable conformance is required by the PP to which conformance is being claimed, the evaluator examines the conformance claim rationale to determine that it demonstrates that the statement of security problem definition of the PP under evaluation is equivalent or more restrictive than the statement of security problem definition in the PP to which conformance is being claimed.

For this, the conformance claim rationale needs to demonstrate that the security problem definition in the PP claiming conformance is equivalent (or more restrictive) than the security problem definition in the PP to which conformance is claimed. This means that:

- all TOEs that would meet the security problem definition in the PP claiming conformance also meet the security problem definition in the PP to which conformance is claimed. This can also be shown indirectly by demonstrating that every event, which realizes a threat defined in the PP to which conformance is

Copyrighted - To reproduction and circulation FOR COCY's review

© ISO/IEC 2022 – All rights reserved
Documents Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

claimed, or violates an OSP defined in the PP to which conformance is claimed, would also realize a threat stated in the PP claiming conformance or violate an OSP defined in the PP claiming conformance. Note that fulfilling an OSP stated in the PP claiming conformance may avert a threat stated in the PP to which conformance is claimed, or that averting a threat stated in the PP claiming conformance may fulfil an OSP stated in the PP to which conformance is claimed, so threats and OSPs can substitute each other;

- all operational environments that would meet the security problem definition in the PP to which conformance is claimed, would also meet the security problem definition in the PP claiming conformance (with one exception in the next bullet);

- besides a set of assumptions in the PP claiming conformance needed to demonstrate conformance to the SPD of the PP to which conformance is claimed, a PP claiming conformance may specify further assumptions, but only if these additional assumptions are independent of and do not affect the security problem definition as defined in the PP to which conformance is claimed. More detailed, there are no assumptions in the PP claiming conformance that exclude threats to the TOE that need to be countered by the TOE according to the PP to which conformance is claimed. Similarly, there are no assumptions in the PP claiming conformance that realize aspects of an OSP stated in the PP to which conformance is claimed, which are meant to be fulfilled by the TOE according to the PP to which conformance is claimed.

ISO/IEC 15408-3:2022 APE_CCL.1.11C: *The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs and any functional packages for which conformance is being claimed.*

10.4.1.3.15 Work unit APE_CCL.1-14

The evaluator ***shall examine*** the conformance claim rationale to determine that the statement of security objectives is consistent with the statement of security objectives in the PPs and functional packages to which conformance is being claimed, taking into consideration the conformance statement of PPs to which conformance is being claimed..

If the PP does not claim conformance to another PP nor to functional packages, this work unit is not applicable and therefore considered to be satisfied.

If conformance is claimed to any functional packages, the evaluator determines that the security objectives of the PP under evaluation include all security objectives of all functional packages to which conformance is claimed.

If packages are used, the rules defined in the following paragraphs concerning strict and demonstrable conformance also hold for the security objectives taken from the packages.

Note that since a PP can only claim conformance to another PP whose conformance statement requires strict or demonstrable conformance, those are the only cases covered in the following paragraphs. If strict conformance is required by the PP to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator determines whether:

a) the PP under evaluation contains all security objectives for the TOE of the PP to which conformance is being claimed. Note that it is allowed for the PP under evaluation to have additional security objectives for the TOE;

b) the security objectives for the operational environment in the PP claiming conformance are identical to the security objectives for the operational environment in the PP to which conformance is being claimed, with two possible exceptions described in the following two bullet points;

c) a security objective for the operational environment (or part of such security objective) from the PP to which conformance is claimed, can be replaced by the same (part of the) security objective stated for the TOE;

Copyrighted - no reproduction and circulation
For CCV's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

d) a security objective for the operational environment can be added to the objectives defined in the PP to which conformance is claimed, if a justification is given, why the new objective neither mitigates a threat (or a part of a threat) meant to be addressed by security objectives for the TOE in the PP to which conformance is claimed, nor fulfils an OSP (or part of an OSP) meant to be addressed by security objectives for the TOE in the PP to which conformance is claimed.

When examining a PP claiming another PP which omits security objectives for the operational environment from the PP to which conformance is claimed, or adds new security objectives for the operational environment, the evaluator shall carefully determine, if the conditions given above are fulfilled. The examples given for the case of assumptions in the preceding work unit are also valid here.

If demonstrable conformance is required by the PP to which conformance is being claimed, the evaluator examines the conformance claim rationale to determine that it demonstrates that the statement of security objectives of the PP under evaluation is equivalent or more restrictive than the statement of security objectives in the PP to which conformance is being claimed.

For this the conformance claim rationale needs to demonstrate that the security objectives in the PP claiming conformance are equivalent to (or more restrictive than) the security objectives in the PP to which conformance is claimed. This means that:

a) all TOEs that would meet the security objectives for the TOE in the PP claiming conformance also meet the security objectives for the TOE in the PP to which conformance is claimed;

b) all operational environments that would meet the security objectives for the operational environment in the PP to which conformance is claimed, would also meet the security objectives for the operational environment in the PP claiming conformance (with one exception in the next bullet);

c) besides a set of security objectives for the operational environment in the PP claiming conformance, which are used to demonstrate conformance to the set of security objectives defined in the PP to which conformance is claimed, a PP claiming conformance may specify further security objectives for the operational environment, but only if these security objectives neither affect the original set of security objectives for the TOE nor the security objectives for the operational environment as defined in the PP to which conformance is claimed.

ISO/IEC 15408-3:2022 APE_CCL.1.12C: *The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs, and any functional packages for which conformance is being claimed.*

10.4.1.3.16 Work unit APE_CCL.1-15

The evaluator ***shall examine*** the PP to determine that the statement of security requirements is consistent with all security requirements stated in the PPs and any functional packages to which conformance is being claimed, taking into consideration the conformance statements of PPs to which conformance is being claimed.

If the PP does not claim conformance to another PP nor to functional packages, this work unit is not applicable and therefore considered to be satisfied.

If conformance is claimed to any functional packages, the evaluator determines that the SFRs of the PP under evaluation include all SFRs (or hierarchical SFRs) of all functional packages to which conformance is claimed.

If packages are used, the rules defined in the following paragraphs concerning strict and demonstrable conformance also hold for the SFRs taken from the packages.

Note that since a PP can only claim conformance to another PP whose conformance statement requires strict or demonstrable conformance, those are the only cases covered in the following paragraphs.

Copyrighted - no reproduction and circulation
For CCV's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

If strict conformance is required by the PP to which conformance is being claimed, no conformance claim rationale is required. Instead, the evaluator determines whether the statement of security requirements in the PP under evaluation is a superset of or identical to the statement of security requirements in the PP to which conformance is being claimed (for strict conformance).

If demonstrable conformance is required by the PP to which conformance is being claimed, the evaluator examines the conformance claim rationale to determine that it demonstrates that the statement of security requirements of the PP under evaluation is equivalent or more restrictive than the statement of security requirements in the PP to which conformance is being claimed.

For:

- SFRs: The conformance rationale in the PP claiming conformance shall demonstrate that the overall set of requirements defined by the SFRs in the PP claiming conformance is equivalent (or more restrictive) than the overall set of requirements defined by the SFRs in the PP to which conformance is claimed. This means that all TOEs that would meet the requirements defined by the set of all SFRs in the PP claiming conformance would also meet the requirements defined by the set of all SFRs in the PP to which conformance is claimed;

- SARs: The PP claiming conformance shall contain all SARs in the PP to which conformance is claimed, but may claim additional SARs or replace SARs by hierarchically stronger SARs. The completion of operations in the PP claiming conformance must be consistent with that in the PP to which conformance is claimed; either the same completion will be used in the PP claiming conformance as that in the PP to which conformance is claimed or a completion that makes the SAR more restrictive (the rules of refinement apply).

ISO/IEC 15408-3:2022 APE_CCL.1.13C: *The conformance statement shall describe the conformance required of any PPs/STs to the PP as exact-PP, strict-PP or demonstrable-PP conformance.*

10.4.1.3.17 Work unit APE_CCL.1-16

The evaluator ***shall check*** that the PP conformance statement states a claim of exact-PP, strict-PP or demonstrable-PP conformance.

ISO/IEC 15408-3:2022 APE_CCL.1.14C: *For an exact conformance PP, the conformance statement shall contain an allowed-with statement that identifies the set of PPs (if any) to which, in combination with the PP under evaluation, exact conformance is allowed to be claimed.*

10.4.1.3.18 Work unit APE_CCL.1-17

The evaluator ***shall check*** the conformance statement to determine that it contains an allowed-with statement that lists the set of PPs to which, in combination with the PP being evaluated, an exact conformance claim (in an ST or PP-Configuration) is allowed.

If the PP does not require exact conformance in its conformance statement, this work unit does not apply and is therefore considered satisfied.

If the PP does not allow claims of exact conformance to it in combination with any other PPs, then no list of PPs is required and this work unit is considered satisfied.

The usage of the allowed-with statement is a matter of policy and is not addressed here. There are no other actions for the evaluator other than determining that the list is present.

ISO/IEC 15408-3:2022 APE_CCL.1.15C: *For an exact conformance PP, the conformance statement shall contain an allowed-with statement that identifies the set of PP-Modules (if any) that are allowed to be used with the PP under evaluation in a PP-Configuration.*

Copyrighted - no reproduction and circulation - For CCCYS review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

10.4.1.3.19 Work unit APE_CCL.1-18

The evaluator ***shall check*** the conformance statement to determine that it contains an allowed-with statement that lists the set of PP-Modules that, in combination with the PP being evaluated, can be present in a PP-Configuration that requires exact conformance.

If the PP does not require exact conformance in its conformance statement, this work unit does not apply and is therefore considered satisfied.

If the PP does not allow claims of exact conformance to it in combination with any PP-Modules, then no list of PP-Modules is required and this work unit is considered satisfied.

The usage of the allowed-with statement is a matter of policy and is not addressed here. There are no other actions for the evaluator other than determining that the list is present.

ISO/IEC 15408-3:2022 APE_CCL.1.16C: *The conformance statement shall identify the set of derived Evaluation Methods and Evaluation Activities (if any) that shall be used with the PP under evaluation. This list shall contain:*

- *any Evaluation Methods and Evaluation Activities that are specified for the PP under evaluation;*
- *any Evaluation Methods and Evaluation Activities specified in conformance statements of PPs to which conformance is being claimed by the PP under evaluation;*
- *any Evaluation Methods and Evaluation Activities specified in the Security Requirements sections of packages to which conformance is being claimed by the PP under evaluation.*

10.4.1.3.20 Work unit APE_CCL.1-19

The evaluator ***shall check*** the conformance statement of the PP under evaluation to determine that:

a) if any derived Evaluation Methods and Evaluation Activities are required by other items to which the PP claims conformance then these are all identified in the PP under evaluation, along with any derived Evaluation Methods and Evaluation Activities that the PP itself requires;

b) the list of derived Evaluation Methods and Evaluation Activities is sufficiently structured and detailed to unambiguously identify and locate every member of the list;

c) if there is any overlap in the scope of the identified Evaluation Methods and Evaluation Activities (i.e. where an overlay exists as described in ISO/IEC 15408-4) then the rationale for the resulting set of Evaluation Methods and Evaluation Activities is applicable to the TOE as described by the PP under evaluation.

The intention of this work unit is to ensure that when evaluating a TOE that claims conformance with the PP under evaluation then the correct Evaluation Methods and Evaluation Activities can be used. This means that identification in the PP need not list individual Evaluation Activities where these are unambiguously included in a listed Evaluation Method. Similarly, where multiple Evaluation Methods or Evaluation Activities are included in a single document then it is sufficient to reference the document, provided this does lead to unambiguous identification of the Evaluation Methods and Evaluation Activities that apply to the PP under evaluation.

EXAMPLE If a document lists multiple different Evaluation Methods applicable to different use cases then it would not be sufficient to reference the document: the relevant use cases would also have to be identified.

Copyrighted - no reproduction and circulation
For CCVS review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

10.5 Security problem definition (APE_SPD)

10.5.1 Evaluation of sub-activity (APE_SPD.1)

10.5.1.1 Objectives

The objective of this sub-activity is to determine that the security problem intended to be addressed by the TOE and its operational environment is clearly defined.

10.5.1.2 Input

The evaluation evidence for this sub-activity is:

a) the PP.

10.5.1.3 Action APE_SPD.1.1E

10.5.1.3.1 General

ISO/IEC 15408-3:2022 APE_SPD.1.1C: *The security problem definition shall describe the threats.*

10.5.1.3.2 Work unit APE_SPD.1-1

The evaluator ***shall check*** that the security problem definition describes the threats.

If all security objectives are derived from assumptions and/or OSPs only, the statement of threats need not be present in the PP. In this case, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that the security problem definition describes the threats that must be countered by the TOE and/or its operational environment.

Note that if optional requirements are defined by the PP, there may be associated threats that are covered by this work unit.

ISO/IEC 15408-3:2022 APE_SPD.1.2C: *All threats shall be described in terms of a threat agent, an asset, and an adverse action.*

10.5.1.3.3 Work unit APE_SPD.1-2

The evaluator ***shall examine*** the security problem definition to determine that all threats are described in terms of a threat agent, an asset, and an adverse action.

If all security objectives are derived from assumptions and OSPs only, the statement of threats need not be present in the PP. In this case, this work unit is not applicable and therefore considered to be satisfied.

Threat agents may be further described by aspects such as expertise, resource, opportunity, and motivation.

ISO/IEC 15408-3:2022 APE_SPD.1.3C: *The security problem definition shall describe the organizational security policies (OSPs).*

10.5.1.3.4 Work unit APE_SPD.1-3

The evaluator ***shall examine*** that the security problem definition describes the OSPs.

If all security objectives are derived from assumptions and/or threats only, OSPs need not be present in the PP. In this case, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that OSP statements are made in terms of rules or guidelines that must be followed by the TOE and/or its operational environment.

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

The evaluator determines that each OSP is explained and/or interpreted in sufficient detail to make it clearly understandable; a clear presentation of policy statements is necessary to permit tracing security objectives to them.

Note that if optional requirements are defined by the PP, there may be associated OSPs that are covered by this work unit.

ISO/IEC 15408-3:2022 APE_SPD.1.4C: *The security problem definition shall describe the assumptions about the operational environment of the TOE.*

10.5.1.3.5 Work unit APE_SPD.1-4

The evaluator ***shall examine*** the security problem definition to determine that it describes the assumptions about the operational environment of the TOE.

If there are no assumptions, this work unit is not applicable and is therefore considered to be satisfied.

The evaluator determines that each assumption about the operational environment of the TOE is explained in sufficient detail to enable consumers to determine that their operational environment matches the assumption. If the assumptions are not clearly understood, the end result may be that the TOE is used in an operational environment in which it will not function in a secure manner.

10.6 Security objectives (APE_OBJ)

10.6.1 Evaluation of sub-activity (APE_OBJ.1)

10.6.1.1 Objectives

The objective of this sub-activity is to determine whether the security objectives for the operational environment are clearly defined.

10.6.1.2 Input

The evaluation evidence for this sub-activity is:

a) the PP.

10.6.1.3 Action APE_OBJ.1.1E

10.6.1.3.1 General

ISO/IEC 15408-3:2022 APE_OBJ.1.1C: *The statement of security objectives shall describe the security objectives for the operational environment.*

10.6.1.3.2 Work unit APE_OBJ.1-1

The evaluator ***shall check*** that the statement of security objectives defines the security objectives for the operational environment.

The evaluator checks that the security objectives for the operational environment are identified.

ISO/IEC 15408-3:2022 APE_OBJ.1.2C: *The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.*

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

10.6.1.3.3 Work unit APE_OBJ.1-2

The evaluator ***shall check*** that the security objectives rationale traces the security objectives for the operational environment back to threats countered by that security objective, to OSPs enforced by that security objective, and to assumptions upheld by that security objective.

Each security objective for the operational environment may trace back to threats, OSPs, assumptions, or a combination of threats, OSPs and/or assumptions, but it must trace back to at least one threat, OSP or assumption.

Failure to trace a security objective for the operational environment back to at least a threat, OSP or assumption, implies that either the security objectives rationale is incomplete, the security problem definition is incomplete, or the security objective for the operational environment has no useful purpose.

There is no prescribed location where this tracing element of the rationale must be placed: for example, the relevant parts may be located under each threat, OSP and assumption in order to help make the security argument clearer and easier to read.

ISO/IEC 15408-3:2022 APE_OBJ.1.3C: *The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.*

10.6.1.3.4 Work unit APE_OBJ.1-3

The evaluator ***shall examine*** the security objectives rationale to determine that for each assumption for the operational environment it contains an appropriate justification that the security objectives for the operational environment are suitable to uphold that assumption.

If no security objectives for the operational environment trace back to the assumption, the evaluator action related to this work unit is assigned a fail verdict.

The evaluator determines that the justification for an assumption about the operational environment of the TOE demonstrates that the security objectives are sufficient: if all security objectives for the operational environment that trace back to that assumption are achieved, the operational environment upholds the assumption.

The evaluator also determines that each security objective for the operational environment that traces back to an assumption about the operational environment of the TOE is necessary: when the security objective is achieved it actually contributes to the operational environment upholding the assumption.

Note that simply listing in the security objectives rationale the security objectives for the operational environment associated with each assumption may be a part of a justification, but does not constitute a justification by itself. A descriptive justification is required, although in simple cases this justification may be as minimal as "Security Objective X directly upholds Assumption Y".

10.6.2 Evaluation of sub-activity (APE_OBJ.2)

10.6.2.1 Objectives

The objective of this sub-activity is to determine whether the security objectives adequately and completely address the security problem definition and that the division of this problem between the TOE and its operational environment is clearly defined.

10.6.2.2 Input

The evaluation evidence for this sub-activity is:

a) the PP.

Copyrighted - no reproduction and circulation
For CCCY's review

© ISO/IEC 2022 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

10.6.2.3 Action APE_OBJ.2.1E

10.6.2.3.1 General

ISO/IEC 15408-3:2022 APE_OBJ.2.1C: *The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.*

10.6.2.3.2 Work unit APE_OBJ.2-1

The evaluator ***shall check*** that the statement of security objectives defines the security objectives for the TOE and the security objectives for the operational environment.

The evaluator checks that both categories of security objectives are clearly identified and separated from the other category.

ISO/IEC 15408-3:2022 APE_OBJ.2.2C: *The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.*

10.6.2.3.3 Work unit APE_OBJ.2-2

The evaluator ***shall check*** that the security objectives rationale traces all security objectives for the TOE back to threats countered by the objectives and/or OSPs enforced by the objectives.

Each security objective for the TOE may trace back to threats or OSPs, or a combination of threats and OSPs, but it must trace back to at least one threat or OSP. Optional requirements may require Threats/OSPs to be specified, and security objectives associated with these SPD elements are also covered by this work unit.

Failure to trace a security objective for the TOE back to at least one threat or OSP, implies that either the security objectives rationale is incomplete, the security problem definition is incomplete, or the security objective for the TOE has no useful purpose.

ISO/IEC 15408-3:2022 APE_OBJ.2.3C: *The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.*

10.6.2.3.4 Work unit APE_OBJ.2-3

The evaluator ***shall check*** that the security objectives rationale traces the security objectives for the operational environment back to threats countered by that security objective, to OSPs enforced by that security objective, and to assumptions upheld by that security objective.

Each security objective for the operational environment may trace back to threats, OSPs, assumptions, or a combination of threats, OSPs and/or assumptions, but it must trace back to at least one threat, OSP or assumption.

Failure to trace a security objective for the operational environment back to at least one threat, OSP, or assumption, implies that either the security objectives rationale is incomplete, the security problem definition is incomplete, or the security objective for the operational environment has no useful purpose.

ISO/IEC 15408-3:2022 APE_OBJ.2.4C: *The security objectives rationale shall demonstrate that the security objectives counter all threats.*

10.6.2.3.5 Work unit APE_OBJ.2-4

The evaluator ***shall examine*** the security objectives rationale to determine that it justifies for each threat that the security objectives are suitable to counter that threat.

If no security objectives trace back to the threat, the evaluator action related to this work unit is assigned a fail verdict.

Copyrighted - no reproduction and circulation
For CCCYS review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022

The evaluator determines that the justification for a threat shows whether the threat is removed, diminished or mitigated.

The evaluator determines that the justification for a threat demonstrates that the security objectives are sufficient: if all security objectives that trace back to the threat are achieved, the threat is removed, sufficiently diminished, or the effects of the threat are sufficiently mitigated.

Note that the tracings from security objectives to threats provided in the security objectives rationale may be part of a justification, but do not constitute a justification by themselves. Even in the case that a security objective is merely a statement reflecting the intent to prevent a particular threat from being realised, a justification is required, but this justification may be as minimal as "Security Objective X directly counters Threat Y".

The evaluator also determines that each security objective that traces back to a threat is necessary: when the security objective is achieved it actually contributes to the removal, diminishing or mitigation of that threat.

ISO/IEC 15408-3:2022 APE_OBJ.2.5C: *The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.*

10.6.2.3.6 Work unit APE_OBJ.2-5

The evaluator ***shall examine*** the security objectives rationale to determine that for each OSP it justifies that the security objectives are suitable to enforce that OSP.

If no security objectives trace back to the OSP, the evaluator action related to this work unit is assigned a fail verdict.

The evaluator determines that the justification for an OSP demonstrates that the security objectives are sufficient: if all security objectives that trace back to that OSP are achieved, the OSP is enforced.

The evaluator also determines that each security objective that traces back to an OSP is necessary: when the security objective is achieved it actually contributes to the enforcement of the OSP.

Note that the tracings from security objectives to OSPs provided in the security objectives rationale may be part of a justification, but do not constitute a justification by themselves. In the case that a security objective is merely a statement reflecting the intent to enforce a particular OSP, a justification is required, but this justification may be as minimal as "Security Objective X directly enforces OSP Y".

ISO/IEC 15408-3:2022 APE_OBJ.2.6C: *The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.*

10.6.2.3.7 Work unit APE_OBJ.2-6

The evaluator ***shall examine*** the security objectives rationale to determine that for each assumption for the operational environment it contains an appropriate justification that the security objectives for the operational environment are suitable to uphold that assumption.

If no security objectives for the operational environment trace back to the assumption, the evaluator action related to this work unit is assigned a fail verdict.

The evaluator determines that the justification for an assumption about the operational environment of the TOE demonstrates that the security objectives are sufficient: if all security objectives for the operational environment that trace back to that assumption are achieved, the operational environment upholds the assumption.

The evaluator also determines that each security objective for the operational environment that traces back to an assumption about the operational environment of the TOE is necessary: when the security objective is achieved it actually contributes to the operational environment upholding the assumption.

Copyrighted - no reproduction and circulation
For CCCY's review

Documents
Document Sharing Hub

© ISO/IEC 2022 – All rights reserved

Full document details: ISO_IEC 18045 (WG)_2022

Note that the tracings from security objectives for the operational environment to assumptions provided in the security objectives rationale may be a part of a justification, but do not constitute a justification by themselves. Even in the case that a security objective of the operational environment is merely a restatement of an assumption, a justification is required, but this justification may be as minimal as "Security Objective X directly upholds Assumption Y".

10.7 Extended components definition (APE_ECD)

10.7.1 Evaluation of sub-activity (APE_ECD.1)

10.7.1.1 Objectives

The objective of this sub-activity is to determine whether extended components have been clearly and unambiguously defined, and whether they are necessary, i.e. they may not be clearly expressed using existing ISO/IEC 15408-2 or ISO/IEC 15408-3 components.

10.7.1.2 Input

The evaluation evidence for this sub-activity is the PP.

10.7.1.3 Action APE_ECD.1.1E

10.7.1.3.1 General

ISO/IEC 15408-3:2022 APE_ECD.1.1C: *The statement of security requirements shall identify all extended security requirements.*

10.7.1.3.2 Work unit APE_ECD.1-1

The evaluator ***shall check*** that all security requirements in the statement of security requirements that are not identified as extended requirements are present in ISO/IEC 15408-2 or in ISO/IEC 15408-3.

ISO/IEC 15408-3:2022 APE_ECD.1.2C: *The extended components definition shall define an extended component for each extended security requirement.*

10.7.1.3.3 Work unit APE_ECD.1-2

The evaluator ***shall check*** that the extended components definition defines an extended component for each extended security requirement.

If the PP does not contain extended security requirements, this work unit is not applicable and therefore considered to be satisfied.

A single extended component may be used to define multiple iterations of an extended security requirement, it is not necessary to repeat this definition for each iteration.

ISO/IEC 15408-3:2022 APE_ECD.1.3C: *The extended components definition shall describe how each extended component is related to the existing ISO/IEC 15408 series components, families, and classes.*

10.7.1.3.4 Work unit APE_ECD.1-3

The evaluator ***shall examine*** the extended components definition to determine that it describes how each extended component fits into the existing ISO/IEC 15408 components, families, and classes.

If the PP does not contain extended security requirements, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that each extended component is either:

Copyrighted - no reproduction and circulation
For CCDB's review

© ISO/IEC 2022 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 18045 (WG)_2022