

DIN EN ISO/IEC 18045



ICS 35.030

Einsprüche bis 2019-12-18

Entwurf

**Informationstechnik –
Sicherheitstechniken –
Methodik für die Bewertung der IT-Sicherheit (ISO/IEC 18045:2008);
Englische Fassung prEN ISO/IEC 18045:2019**

Information technology –
Security techniques –
Methodology for IT security evaluation (ISO/IEC 18045:2008);
English version prEN ISO/IEC 18045:2019

Technologies de l'information –
Techniques de sécurité –
Méthodologie pour l'évaluation de sécurité TI (ISO/IEC 18045:2008);
Version anglaise prEN ISO/IEC 18045:2019

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2019-10-18 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an nia@din.de möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an den DIN-Normenausschuss Informationstechnik und Anwendungen (NIA), 10772 Berlin, Saatwinkler Damm 42/43, 13627 Berlin.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 304 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 18045:2008 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 18045:2019 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Gremium ist der Arbeitskreis NA 043-01-27-03 AK „Evaluationskriterien für IT-Sicherheit“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Dieses Dokument enthält unter Berücksichtigung des Präsidialbeschlusses 1/2004 nur die englische Originalfassung der ISO/IEC-Norm.

Nationaler Anhang NA (informativ)

Begriffe

Die Benummerung der folgenden Begriffe und Abkürzungen sind identisch mit der Benummerung in der englischen Fassung.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ANMERKUNG Für fettgedruckte Begriffe ist in diesem Unterabschnitt eine eigene Definition aufgeführt.

3.1

Aktion

Evaluatoren-Aktionselement aus ISO/IEC 15408-3

ANMERKUNG Diese Aktionen werden entweder explizit als Evaluatorenaktionen angegeben oder implizit aus Entwickleraktionen (implizite Evaluatorenaktionen) innerhalb der Vertrauenswürdigkeitskomponenten in ISO/IEC 15408-3 abgeleitet.

3.2

Aufgabe

Anwendung einer Vertrauenswürdigkeitsklasse aus ISO/IEC 15408-3

3.3

prüfen

auf Grundlage eines einfachen Vergleichs eine **Entscheidung** treffen

ANMERKUNG Fachwissen eines Evaluatoren ist nicht erforderlich. Eine Aussage, die dieses Verb verwendet, beschreibt eine Zuordnung.

3.4

Evaluationsbeitrag

Ressource, die der Evaluator oder die Evaluierungsinstanz vom Antragsteller oder Entwickler anfordert, um eine oder mehrere Evaluierungsaufgaben oder Evaluierungsüberwachungsaufgaben auszuführen

3.5

Evaluationsnachweis

konkreter **Evaluationsbeitrag**

3.6

Technischer Evaluierungsbericht

Bericht, in dem die vom Evaluator erstellte und bei einer Evaluierungsinstanz eingereichte **Gesamtentscheidung** einschließlich Begründung dokumentiert ist

3.7

untersuchen

mittels Analyse und unter Nutzung von Evaluatoren-Fachwissen eine **Entscheidung** treffen

ANMERKUNG Eine Aussage, die dieses Verb verwendet, nennt die analysierten Sachverhalte und die Eigenschaften, aufgrund derer die Analyse durchgeführt wurde.

3.8

Interpretation

Klarstellung oder Erweiterung einer Anforderung aus ISO/IEC 15408, ISO/IEC 18045 oder aus dem **Schema**

3.9

Methodologie

System aus Vorgehensweisen, Verfahren und Prozessen, das für die IT-Sicherheitsevaluierung verwendet wird

3.10

Beobachtungsbericht

Bericht, der vom Evaluator verfasst wird, wenn dieser während der Evaluierung eine Klarstellung benötigt oder ein Problem identifiziert hat

3.11

Gesamtentscheidung

Urteil „akzeptiert“ oder „abgelehnt“, das ein Evaluator ausgehend vom Ergebnis einer Evaluierung fällt

3.12

Überwachungsentscheidung

Urteil, das von einer Evaluierungsinstanz gefällt wird und mit dem diese eine *Gesamtentscheidung* auf Grundlage der Ergebnisse von Evaluierungsüberwachungsaufgaben bestätigt oder ablehnt

3.13

aufzeichnen

eine Beschreibung der Verfahren, Ereignisse, Beobachtungen, Erkenntnisse und Ergebnisse schriftlich festhalten, die so detailliert ist, dass die für die Evaluierung ausgeführten Arbeitsschritte damit zu einem späteren Zeitpunkt rekonstruiert werden können

3.14

berichten

Evaluierungsergebnisse und dokumentierende Angaben und Unterlagen im **Technischen Evaluierungsbericht** oder einem **Beobachtungsbericht** zusammenstellen

3.15

Schema

Reihe von Regeln, die eine Evaluierungsinstanz zur Definition der Evaluierungsumgebung festlegt, einschließlich der für die Durchführung von IT-Sicherheitsevaluierungen erforderlichen Kriterien und **Methodologie**

3.16

Unteraufgabe

Anwendung einer Vertrauenswürdigkeitskomponente aus ISO/IEC 15408-3

ANMERKUNG Vertrauenswürdigkeitsfamilien werden in dieser Internationalen Norm nicht explizit behandelt, da Evaluierungen an einer einzelnen Vertrauenswürdigkeitskomponente aus einer Vertrauenswürdigkeitsfamilie durchgeführt werden.

3.17

Verfolgung

einfache direktionale Beziehung zwischen zwei Sätzen von Entitäten, die zeigt, welche Entitäten des ersten Satzes welchen Entitäten des zweiten Satzes entsprechen

3.18

Entscheidung

Urteil „akzeptiert“, „abgelehnt“ oder „nicht bewertbar“, das ein Evaluator hinsichtlich eines Evaluatoren-Aktionselements oder einer Vertrauenswürdigkeitskomponente oder -klasse fällt

ANMERKUNG Siehe auch **Gesamtentscheidung**.

3.19

Workunit

Ebene der kleinsten Einheiten bei der Durchführung der Evaluierung

ANMERKUNG Jede Aktion der Evaluierungsmethodologie umfasst eine oder mehrere Workunits, die innerhalb dieser Aktion nach ihrem ISO/IEC 15408-Inhalt und Nachweisdarstellung oder dem Entwickler-Aktionselement gruppiert wird/werden. Die Workunits werden in dieser Internationalen Norm in der gleichen Reihenfolge dargestellt, wie die Elemente in ISO/IEC 15408, von denen sie abgeleitet wurden. Workunits sind am linken Rand durch eine Zeichenkette gekennzeichnet, z. B. als „ALC_TAT.1-2“. Bei dieser Zeichenkette gibt die Zeichenfolge *ALC_TAT.1* an, um welche Komponente nach ISO/IEC 15408 es sich handelt (d. h., die Unteraufgabe in dieser Internationalen Norm), während die letzte Ziffer (2) anzeigt, dass es sich hierbei um die zweite Workunit der Unteraufgabe ALC_TAT.1 handelt.

— Leerseite —

Contents

Page

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

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

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

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

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

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

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

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

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

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

Legal Notice

The governmental organizations listed below contributed to the development of this version of the Common Methodology for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Methodology for Information Technology Security Evaluations, version 3.1 (called CEM 3.1), they hereby grant non-exclusive license to ISO/IEC to use CEM 3.1 in the continued development/maintenance of the ISO/IEC 18045 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CEM 3.1 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;
France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;
Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

Introduction

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

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

- Entwurf -

Information technology — Security techniques — Methodology for IT security evaluation

1 Scope

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

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

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

3 Terms and definitions

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

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

3.1

action

evaluator action element of ISO/IEC 15408-3

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

3.2

activity

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

3.3

check

generate a **verdict** by a simple comparison

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

3.4

evaluation deliverable

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

3.5

evaluation evidence

tangible **evaluation deliverable**

3.6

evaluation technical report

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

3.7

examine

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

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

3.8

interpretation

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

3.9

methodology

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

3.10

observation report

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

3.11

overall verdict

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

3.12

oversight verdict

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

3.13

record

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

3.14

report

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

3.15

scheme

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

3.16

sub-activity

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

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

3.17

tracing

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

3.18

verdict

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

NOTE Also see **overall verdict**.

3.19

work unit

most granular level of evaluation work

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

4 Symbols and abbreviated terms

ETR **Evaluation Technical Report**

OR Observation Report

5 Overview

5.1 Organisation of this International Standard

Clause 6 defines the conventions used in this International Standard.

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

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

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

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

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

6 Document Conventions

6.1 Terminology

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

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

6.2 Verb usage

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

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 when the described method is strongly preferred. All other auxiliary verbs, including *may*, are used where the described method(s) is allowed but is neither recommended nor strongly preferred; it is merely explanation.

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

6.3 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.

6.4 Relationship between ISO/IEC 15408 and ISO/IEC 18045 structures

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

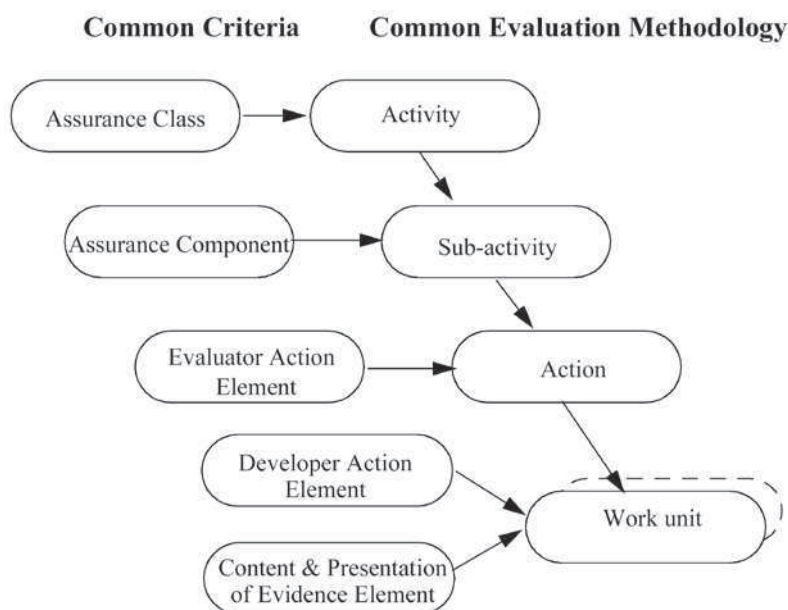


Figure 1 - Mapping of ISO/IEC 15408 and ISO/IEC 18045 structures

7 Evaluation process and related tasks

7.1 Introduction

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 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.

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, and are normative for all ISO/IEC 15408 evaluations (evaluation of a PP or a TOE).

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

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 comply with this International Standard.

The demonstration of the technical competence to the evaluation authority task may 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 Annex 0.

7.2 Evaluation process overview

7.2.1 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.

7.2.2 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.

7.2.3 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 may 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.

7.2.4 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.

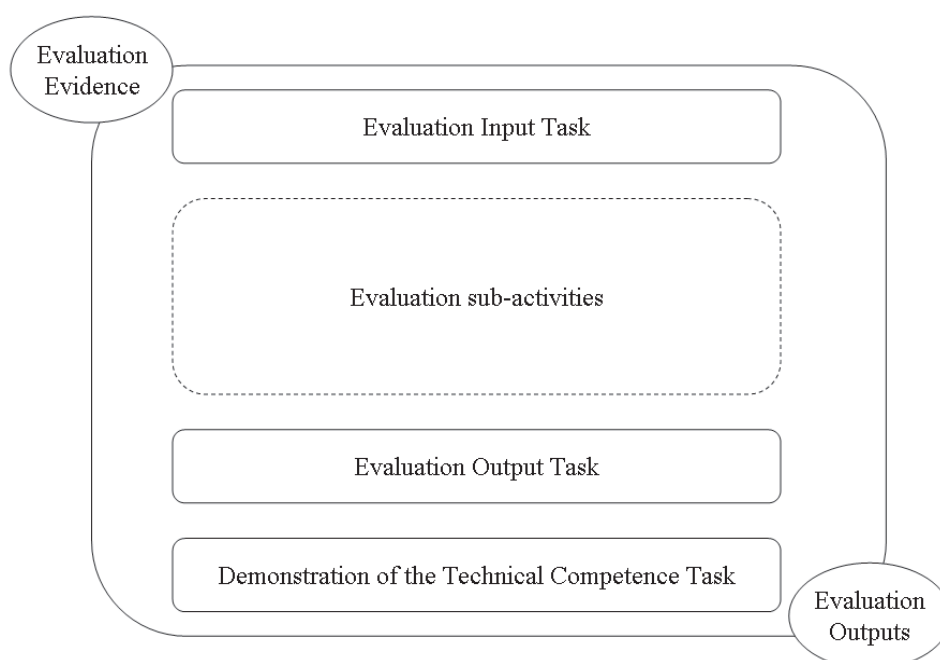


Figure 2 - Generic evaluation model

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.

7.2.5 Evaluator verdicts

The evaluator assigns verdicts to the requirements of ISO/IEC 15408 and not to those of this International Standard. 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. Finally, an evaluation result is assigned, as described in ISO/IEC 15408-1, Clause 9, Evaluation results.

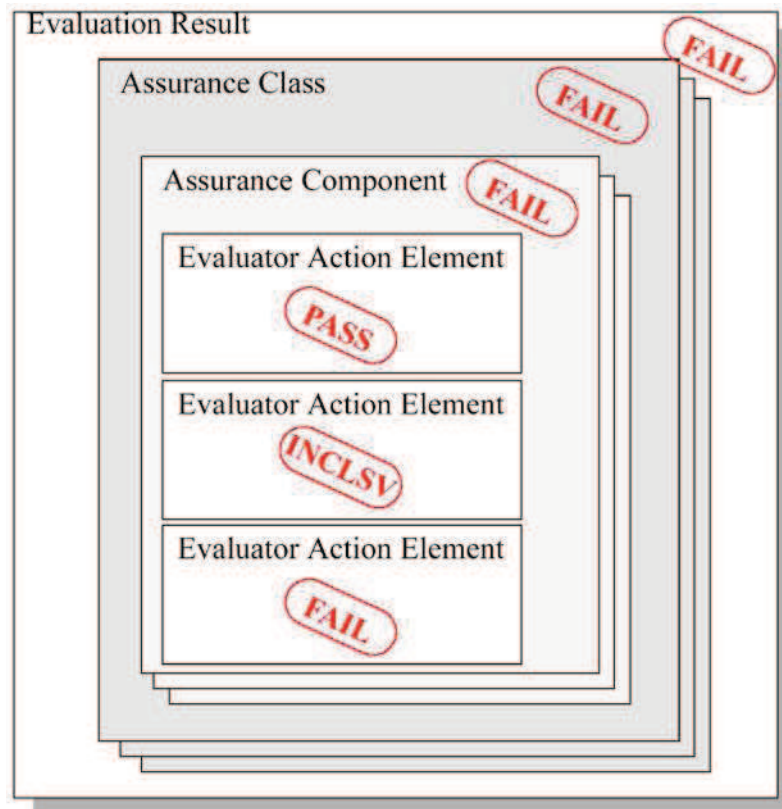


Figure 3 - Example of the verdict assignment rule

This International Standard 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, 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.
- 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, 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*.

7.3 Evaluation input task

7.3.1 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.

7.3.2 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 (for example, 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 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).

7.3.3 Management of evaluation evidence sub-task

7.3.3.1 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.

7.3.3.2 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.

7.3.3.3 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.

7.4 Evaluation sub-activities

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

7.5 Evaluation output task

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

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

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

7.5.2 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.

7.5.3 Application notes

In this version of this International Standard, 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.

7.5.4 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).

7.5.5 Write ETR sub-task

7.5.5.1 Objectives

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

This International Standard 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 International Standard, 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 International Standard.

7.5.5.2 ETR for a PP Evaluation

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.

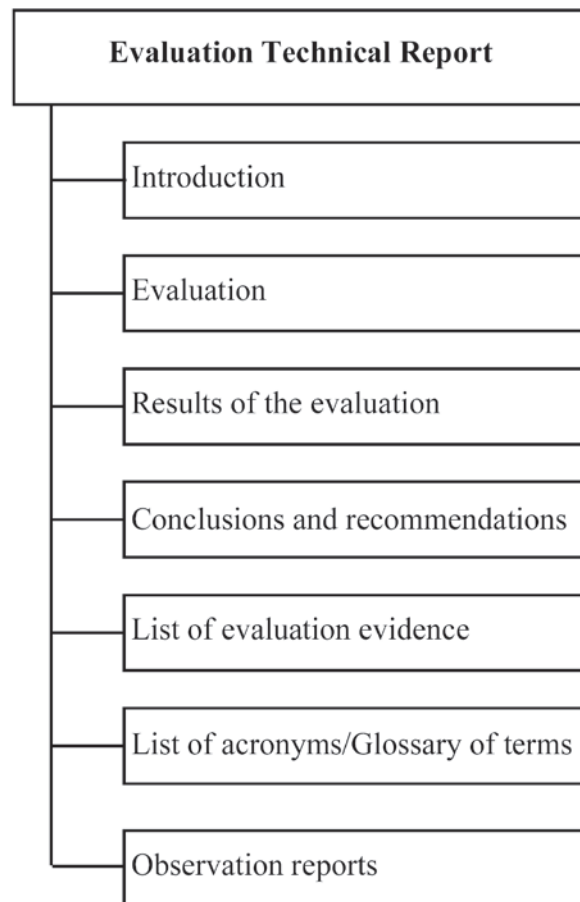


Figure 4 - ETR information content for a PP evaluation

7.5.5.2.1 Introduction

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 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.

7.5.5.2.2 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, etc.

7.5.5.2.3 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 International Standard, 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 a evaluation methodology work unit.

7.5.5.2.4 Conclusions and recommendations

The evaluator **shall report** the conclusions of the evaluation, in particular the overall verdict as defined in ISO/IEC 15408-1 Clause 9, Evaluation results, and determined by application of the verdict assignment described in 7.2.5.

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.

7.5.5.2.5 List of evaluation evidence

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

- the issuing body (e.g. the developer, the sponsor);
- the title;
- the unique reference (e.g. issue date and version number).

7.5.5.2.6 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 International Standard need not be repeated in the ETR.

7.5.5.2.7 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.

7.5.5.3 ETR for a TOE Evaluation

This Subclause describes the minimum content of the ETR for a TOE 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.

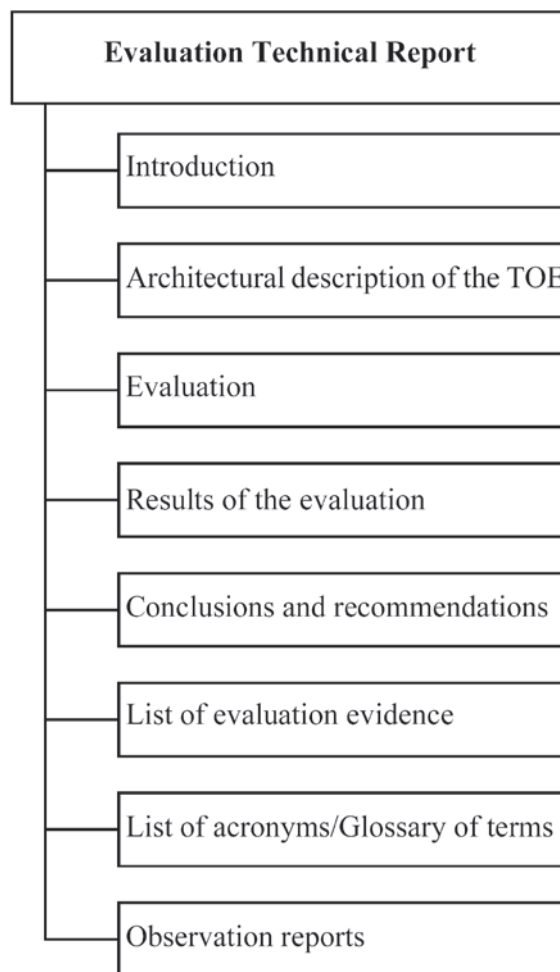


Figure 5 - ETR information content for a TOE evaluation

7.5.5.3.1 Introduction

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, the ETR shall report the reference of the corresponding PPs.

The PPs reference contains information that uniquely identifies the PPs (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.

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.

7.5.5.3.2 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.

7.5.5.3.3 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.

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, etc.

7.5.5.3.4 Results of the evaluation

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

- the title of the activity considered;
- 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 International Standard, 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 a 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.

7.5.5.3.5 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 Clause 9, Evaluation results, and determined by application of the verdict assignment described in 7.2.5.

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.

7.5.5.3.6 List of evaluation evidence

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

- the issuing body (e.g. the developer, the sponsor);
- the title;
- the unique reference (e.g. issue date and version number).

7.5.5.3.7 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 or by this International Standard need not be repeated in the ETR.

7.5.5.3.8 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.

8 Class APE: Protection Profile evaluation

8.1 Introduction

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 class APE.

This Clause should be used in conjunction with Annexes A, B and C, Guidance for Operations in ISO/IEC 15408-1, as these Annexes clarify the concepts here and provide many examples.

8.2 Application notes

8.2.1 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.

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

8.3 PP introduction (APE_INT)

8.3.1 Evaluation of sub-activity (APE_INT.1)

8.3.1.1 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.

8.3.1.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.3.1.3 Action APE_INT.1.1E

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

8.3.1.3.1 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 APE_INT.1.2C: *The PP reference shall uniquely identify the PP.*

8.3.1.3.2 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 APE_INT.1.3C: *The TOE overview shall summarise the usage and major security features of the TOE.*

8.3.1.3.3 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 APE_INT.1.4C: *The TOE overview shall identify the TOE type.*

8.3.1.3.4 Work unit APE_INT.1-4

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

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

8.3.1.3.5 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.

8.4 Conformance claims (APE_CCL)

8.4.1 Evaluation of sub-activity (APE_CCL.1)

8.4.1.1 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.

8.4.1.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP;
- b) the PP(s) that the PP claims conformance to;

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

8.4.1.3 Action APE_CCL.1.1E

ISO/IEC 15408-3 APE_CCL.1.1C: *The conformance claim shall contain an ISO/IEC 15408 conformance claim that identifies the version of ISO/IEC 15408 to which the PP claims conformance.*

8.4.1.3.1 Work unit APE_CCL.1-1

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

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

ISO/IEC 15408-3 APE_CCL.1.2C: *ISO/IEC 15408 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.*

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

8.4.1.3.3 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 conformant or ISO/IEC 15408-3 extended for the PP.

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

8.4.1.3.4 Work unit APE_CCL.1-4

The evaluator **shall examine** 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.

8.4.1.3.5 Work unit APE_CCL.1-5

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

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

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

8.4.1.3.6 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.

8.4.1.3.7 Work unit APE_CCL.1-7

The evaluator **shall check** that the conformance claim contains a package claim that identifies all packages to which the PP claims conformance.

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

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

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

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

8.4.1.3.8 Work unit APE_CCL.1-8

The evaluator **shall check** that, for each identified package, the conformance claim states a claim of either package-name conformant or package-name augmented.

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

If the package conformance claim contains package-name conformant, the evaluator determines that:

- a) If the package is an assurance package, then the PP contains all SARs included in the package, but no additional SARs.
- b) If the package is a functional package, then the PP contains all SFRs included in the package, but no additional SFRs.

If the package conformance claim contains package-name augmented, the evaluator determines that:

- a) If the package is an assurance package, then 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.
- b) If the package is a functional package, then the PP contains all SFRs included in the package, and at least one additional SFR or at least one SFR that is hierarchical to a SFR in the package.

ISO/IEC 15408-3 APE_CCL.1.7C: *The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.*

8.4.1.3.9 Work unit APE_CCL.1-9

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.

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 APE_CCL.1.8C: *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 for which conformance is being claimed.*

8.4.1.3.10 Work unit APE_CCL.1-10

The evaluator **shall examine** the conformance claim rationale to determine that it demonstrates that the statement of security problem definition is consistent, as defined by the conformance statement of the PP, with the statements of security problem definition stated in the PPs to which conformance is being claimed.

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

If the PP to which conformance is being claimed does not have a statement of security problem definition, this work unit is not applicable and therefore considered to be satisfied.

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 fulfills 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, which omits assumptions from another PP to which conformance is claimed, or adds new assumptions, the evaluator shall carefully determine, if the conditions given above are fulfilled. The following discussion gives some motivation and examples for these cases:

- 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 fulfills 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 fulfills 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 fulfill 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 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 fulfill 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, an 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 APE_CCL.1.9C: *The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.*

8.4.1.3.11 Work unit APE_CCL.1-11

The evaluator **shall examine** the conformance claim rationale to determine that the statement of security objectives is consistent, as defined by the conformance statement of the PPs, with the statement of security objectives in the PPs.

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

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 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;
- 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;
- 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;
- 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 fulfills 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 (or more restrictive) than the security objectives in the PP to which conformance is claimed. This means that:

- 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;
- 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);
- 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, an 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 APE_CCL.1.10C: *The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.*

8.4.1.3.12 Work unit APE_CCL.1-12

The evaluator **shall examine** the PP to determine that it is consistent, as defined by the conformance statement of the PP, with all security requirements in the PPs for which conformance is being claimed.

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

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 APE_CCL.1.11C: *The conformance statement shall describe the conformance required of any PPs/STs to the PP as strict-PP or demonstrable-PP conformance.*

8.4.1.3.13 Work unit APE_CCL.1-13

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

8.5 Security problem definition (APE_SPD)

8.5.1 Evaluation of sub-activity (APE_SPD.1)

8.5.1.1 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.

8.5.1.2 Input

The evaluation evidence for this sub-activity is:

a) the PP.

8.5.1.3 Action APE_SPD.1.1E

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

8.5.1.3.1 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.

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

8.5.1.3.2 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 APE_SPD.1.3C: *The security problem definition shall describe the OSPs.*

8.5.1.3.3 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.

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.

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

8.5.1.3.4 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.

8.6 Security objectives (APE_OBJ)

8.6.1 Evaluation of sub-activity (APE_OBJ.1)

8.6.1.1 Objectives

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

8.6.1.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.6.1.3 Action APE_OBJ.1.1E

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

8.6.1.3.1 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.

8.6.2 Evaluation of sub-activity (APE_OBJ.2)

8.6.2.1 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.

8.6.2.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.6.2.3 Action APE_OBJ.2.1E

ISO/IEC 15408-3 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.*

8.6.2.3.1 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 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.*

8.6.2.3.2 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.

Failure to trace 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 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.*

8.6.2.3.3 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 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 APE_OBJ.2.4C: *The security objectives rationale shall demonstrate that the security objectives counter all threats.*

8.6.2.3.4 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.

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 APE_OBJ.2.5C: *The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.*

8.6.2.3.5 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 APE_OBJ.2.6C: *The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.*

8.6.2.3.6 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.

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”.

8.7 Extended components definition (APE_ECD)

8.7.1 Evaluation of sub-activity (APE_ECD.1)

8.7.1.1 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.

8.7.1.2 Input

The evaluation evidence for this sub-activity is:

a) the PP.

8.7.1.3 Action APE_ECD.1.1E

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

8.7.1.3.1 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 APE_ECD.1.2C: *The extended components definition shall define an extended component for each extended security requirement.*

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

8.7.1.3.3 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:

- a) a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 family, or
- b) a member of a new family defined in the PP.

If the extended component is a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 family, the evaluator determines that the extended components definition adequately describes why the extended component should be a member of that family and how it relates to other components of that family.

If the extended component is a member of a new family defined in the PP, the evaluator confirms that the extended component is not appropriate for an existing family.

If the PP defines new families, the evaluator determines that each new family is either:

- a) a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 class, or
- b) a member of a new class defined in the PP.

If the family is a member of an existing ISO/IEC 15408-2 or ISO/IEC 15408-3 class, the evaluator determines that the extended components definition adequately describes why the family should be a member of that class and how it relates to other families in that class.

If the family is a member of a new class defined in the PP, the evaluator confirms that the family is not appropriate for an existing class.

8.7.1.3.4 Work unit APE_ECD.1-4

The evaluator **shall examine** the extended components definition to determine that each definition of an extended component identifies all applicable dependencies of that component.

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

The evaluator confirms that no applicable dependencies have been overlooked by the PP author.

ISO/IEC 15408-3 APE_ECD.1.4C: *The extended components definition shall use the existing ISO/IEC 15408 components, families, classes, and methodology as a model for presentation.*

8.7.1.3.5 Work unit APE_ECD.1-5

The evaluator **shall examine** the extended components definition to determine that each extended functional component uses the existing ISO/IEC 15408-2 components as a model for presentation.

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

The evaluator determines that the extended functional component is consistent with ISO/IEC 15408-2 Subclause 6.1.3, Component structure.

If the extended functional component uses operations, the evaluator determines that the extended functional component is consistent with ISO/IEC 15408-1 Subclause 7.1, Operations.

If the extended functional component is hierarchical to an existing functional component, the evaluator determines that the extended functional component is consistent with ISO/IEC 15408-2 Subclause 6.2.1, Component changes highlighting.

8.7.1.3.6 Work unit APE_ECD.1-6

The evaluator **shall examine** the extended components definition to determine that each definition of a new functional family uses the existing ISO/IEC 15408 functional families as a model for presentation.

If the PP does not define new functional families, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that all new functional families are defined consistent with ISO/IEC 15408-2 Subclause 6.1.2, Family structure.

8.7.1.3.7 Work unit APE_ECD.1-7

The evaluator **shall examine** the extended components definition to determine that each definition of a new functional class uses the existing ISO/IEC 15408 functional classes as a model for presentation.

If the PP does not define new functional classes, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that all new functional classes are defined consistent with ISO/IEC 15408-2 Subclause 6.1.1, Class structure

8.7.1.3.8 Work unit APE_ECD.1-8

The evaluator **shall examine** the extended components definition to determine that each definition of an extended assurance component uses the existing ISO/IEC 15408-3 components as a model for presentation.

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

The evaluator determines that the extended assurance component definition is consistent with ISO/IEC 15408-3 Subclause 6.1.3, Assurance component structure.

If the extended assurance component uses operations, the evaluator determines that the extended assurance component is consistent with ISO/IEC 15408-1 Subclause 7.1, Operations.

If the extended assurance component is hierarchical to an existing assurance component, the evaluator determines that the extended assurance component is consistent with ISO/IEC 15408-3 Subclause 6.1.3, Assurance component structure.

8.7.1.3.9 Work unit APE_ECD.1-9

The evaluator **shall examine** the extended components definition to determine that, for each defined extended assurance component, applicable methodology has been provided.

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

The evaluator determines that, for each evaluator action element of each extended SAR, one or more work units are provided and that successfully performing all work units for a given evaluator action element will demonstrate that the element has been achieved.

8.7.1.3.10 Work unit APE_ECD.1-10

The evaluator **shall examine** the extended components definition to determine that each definition of a new assurance family uses the existing ISO/IEC 15408 assurance families as a model for presentation.

If the PP does not define new assurance families, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that all new assurance families are defined consistent with ISO/IEC 15408-3 Subclause 6.1.2, Assurance family structure.

8.7.1.3.11 Work unit APE_ECD.1-11

The evaluator **shall examine** the extended components definition to determine that each definition of a new assurance class uses the existing ISO/IEC 15408 assurance classes as a model for presentation.

If the PP does not define new assurance classes, this work unit is not applicable and therefore considered to be satisfied.

The evaluator determines that all new assurance classes are defined consistent with ISO/IEC 15408-3 Subclause 6.1.1, Assurance class structure.

ISO/IEC 15408-3 APE_ECD.1.5C: *The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.*

8.7.1.3.12 Work unit APE_ECD.1-12

The evaluator **shall examine** the extended components definition to determine that each element in each extended component is measurable and states objective evaluation requirements, such that conformance or nonconformance can be demonstrated.

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 elements of extended functional components are stated in such a way that they are testable, and traceable through the appropriate TSF representations.

The evaluator also determines that elements of extended assurance components avoid the need for subjective evaluator judgement.

The evaluator is reminded that whilst being measurable and objective is appropriate for all evaluation criteria, it is acknowledged that no formal method exists to prove such properties. Therefore the existing ISO/IEC 15408 functional and assurance components are to be used as a model for determining what constitutes conformance to this requirement.

8.7.1.4 Action APE_ECD.1.2E

8.7.1.4.1 Work unit APE_ECD.1-13

The evaluator **shall examine** the extended components definition to determine that each extended component may not be clearly expressed using existing components.

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

The evaluator should take components from ISO/IEC 15408-2 and ISO/IEC 15408-3, other extended components that have been defined in the PP, combinations of these components, and possible operations on these components into account when making this determination.

The evaluator is reminded that the role of this work unit is to preclude unnecessary duplication of components, that is, components that may be clearly expressed by using other components. The evaluator should not undertake an exhaustive search of all possible combinations of components including operations in an attempt to find a way to express the extended component by using existing components.

8.8 Security requirements (APE_REQ)

8.8.1 Evaluation of sub-activity (APE_REQ.1)

8.8.1.1 Objectives

The objective of this sub-activity is to determine whether the SFRs and SARs are clear, unambiguous and well-defined and whether they are internally consistent.

8.8.1.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.8.1.3 Action APE_REQ.1.1E

ISO/IEC 15408-3 APE_REQ.1.1C: *The statement of security requirements shall describe the SFRs and the SARs.*

8.8.1.3.1 Work unit APE_REQ.1-1

The evaluator **shall check** that the statement of security requirements describes the SFRs.

The evaluator determines that each SFR is identified by one of the following means:

- a) by reference to an individual component in ISO/IEC 15408-2;
- b) by reference to an extended component in the extended components definition of the PP;
- c) by reference to a PP that the PP claims to be conformant with;
- d) by reference to a security requirements package that the PP claims to be conformant with;
- e) by reproduction in the PP.

It is not required to use the same means of identification for all SFRs.

8.8.1.3.2 Work unit APE_REQ.1-2

The evaluator **shall check** that the statement of security requirements describes the SARs.

The evaluator determines that each SAR is identified by one of the following means:

- a) by reference to an individual component in ISO/IEC 15408-3;
- b) by reference to an extended component in the extended components definition of the PP;
- c) by reference to a PP that the PP claims to be conformant with;
- d) by reference to a security requirements package that the PP claims to be conformant with;
- e) by reproduction in the PP.

It is not required to use the same means of identification for all SARs.

ISO/IEC 15408-3 APE_REQ.1.2C: *All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.*

8.8.1.3.3 Work unit APE_REQ.1-3

The evaluator **shall examine** the PP to determine that all subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs are defined.

The evaluator determines that the PP defines all:

- (types of) subjects and objects that are used in the SFRs;

- (types of) security attributes of subjects, users, objects, information, sessions and/or resources, possible values that these attributes may take and any relations between these values (e.g. top_secret is “higher” than secret);
- (types of) operations that are used in the SFRs, including the effects of these operations;
- (types of) external entities in the SFRs;
- other terms that are introduced in the SFRs and/or SARs by completing operations, if these terms are not immediately clear, or are used outside their dictionary definition.

The goal of this work unit is to ensure that the SFRs and SARs are well-defined and that no misunderstanding may occur due to the introduction of vague terms. This work unit should not be taken into extremes, by forcing the PP writer to define every single word. The general audience of a set of security requirements should be assumed to have a reasonable knowledge of IT, security and “Evaluation criteria for IT security”.

All of the above may be presented in groups, classes, roles, types or other groupings or characterisations that allow easy understanding.

The evaluator is reminded that these lists and definitions do not have to be part of the statement of security requirements, but may be placed (in part or in whole) in different subclauses. This may be especially applicable if the same terms are used in the rest of the PP.

ISO/IEC 15408-3 APE_REQ.1.3C: *The statement of security requirements shall identify all operations on the security requirements.*

8.8.1.3.4 Work unit APE_REQ.1-4

The evaluator **shall check** that the statement of security requirements identifies all operations on the security requirements.

The evaluator determines that all operations are identified in each SFR or SAR where such an operation is used. This includes both completed operations and uncompleted operations. Identification may be achieved by typographical distinctions, or by explicit identification in the surrounding text, or by any other distinctive means.

ISO/IEC 15408-3 APE_REQ.1.4C: *All operations shall be performed correctly.*

8.8.1.3.5 Work unit APE_REQ.1-5

The evaluator **shall examine** the statement of security requirements to determine that all assignment operations are performed correctly.

Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C, Guidance for Operations.

8.8.1.3.6 Work unit APE_REQ.1-6

The evaluator **shall examine** the statement of security requirements to determine that all iteration operations are performed correctly.

Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C, Guidance for Operations.

8.8.1.3.7 Work unit APE_REQ.1-7

The evaluator **shall examine** the statement of security requirements to determine that all selection operations are performed correctly.

Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C, Guidance for Operations.

8.8.1.3.8 Work unit APE_REQ.1-8

The evaluator **shall examine** the statement of security requirements to determine that all refinement operations are performed correctly.

Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C, Guidance for Operations.

ISO/IEC 15408-3 APE_REQ.1.5C: *Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.*

8.8.1.3.9 Work unit APE_REQ.1-9

The evaluator **shall examine** the statement of security requirements to determine that each dependency of the security requirements is either satisfied, or that the security requirements rationale justifies the dependency not being satisfied.

A dependency is satisfied by the inclusion of the relevant component (or one that is hierarchical to it) within the statement of security requirements. The component used to satisfy the dependency should, if necessary, be modified by operations to ensure that it actually satisfies that dependency.

A justification that a dependency is not met should address either:

- a) why the dependency is not necessary or useful, in which case no further information is required; or
- b) that the dependency has been addressed by the operational environment of the TOE, in which case the justification should describe how the security objectives for the operational environment address this dependency.

ISO/IEC 15408-3 APE_REQ.1.6C: *The statement of security requirements shall be internally consistent.*

8.8.1.3.10 Work unit APE_REQ.1-10

The evaluator **shall examine** the statement of security requirements to determine that it is internally consistent.

The evaluator determines that the combined set of all SFRs and SARs is internally consistent.

The evaluator determines that on all occasions where different security requirements apply to the same types of developer evidence, events, operations, data, tests to be performed etc. or to “all objects”, “all subjects” etc., that these requirements do not conflict.

Some possible conflicts are:

- a) an extended SAR specifying that the design of a certain cryptographic algorithm is to be kept secret, and another extended SAR specifying an open source review;
- b) FAU_GEN.1 Audit data generation specifying that subject identity is to be logged, FDP_ACC.1 Subset access control specifying who has access to these logs, and FPR_UNO.1 Unobservability specifying that some actions of subjects should be unobservable to other subjects. If the subject that should not be able to see an activity may access logs of this activity, these SFRs conflict;
- c) FDP_RIP.1 Subset residual information protection specifying deletion of information no longer needed, and FDP_ROL.1 Basic rollback specifying that a TOE may return to a previous state. If the information that is needed for the rollback to the previous state has been deleted, these requirements conflict;

- d) Multiple iterations of FDP_ACC.1 Subset access control especially where some iterations cover the same subjects, objects, or operations. If one access control SFR allows a subject to perform an operation on an object, while another access control SFR does not allow this, these requirements conflict.

8.8.2 Evaluation of sub-activity (APE_REQ.2)

8.8.2.1 Objectives

The objective of this sub-activity is to determine whether the SFRs and SARs are clear, unambiguous and well-defined, whether they are internally consistent, and whether the SFRs meet the security objectives of the TOE.

8.8.2.2 Input

The evaluation evidence for this sub-activity is:

- a) the PP.

8.8.2.3 Action APE_REQ.2.1E

ISO/IEC 15408-3 APE_REQ.2.1C: *The statement of security requirements shall describe the SFRs and the SARs.*

8.8.2.3.1 Work unit APE_REQ.2-1

The evaluator **shall check** that the statement of security requirements describes the SFRs.

The evaluator determines that each SFR is identified by one of the following means:

- a) by reference to an individual component in ISO/IEC 15408-2;
- b) by reference to an extended component in the extended components definition of the PP;
- c) by reference to an individual component in a PP that the PP claims to be conformant with;
- d) by reference to an individual component in a security requirements package that the PP claims to be conformant with;
- e) by reproduction in the PP.

It is not required to use the same means of identification for all SFRs.

8.8.2.3.2 Work unit APE_REQ.2-2

The evaluator **shall check** that the statement of security requirements describes the SARs.

The evaluator determines that each SAR is identified by one of the following means:

- a) by reference to an individual component in ISO/IEC 15408-3;
- b) by reference to an extended component in the extended components definition of the PP;
- c) by reference to an individual component in a PP that the PP claims to be conformant with;
- d) by reference to an individual component in a security requirements package that the PP claims to be conformant with;
- e) by reproduction in the PP.

It is not required to use the same means of identification for all SARs.

ISO/IEC 15408-3 APE_REQ.2.2C: *All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.*

8.8.2.3.3 Work unit APE_REQ.2-3

The evaluator **shall examine** the PP to determine that all subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs are defined.

The evaluator determines that the PP defines all:

- (types of) subjects and objects that are used in the SFRs;
- (types of) security attributes of subjects, users, objects, information, sessions and/or resources, possible values that these attributes may take and any relations between these values (e.g. top_secret is “higher” than secret);
- (types of) operations that are used in the SFRs, including the effects of these operations;
- (types of) external entities in the SFRs;
- other terms that are introduced in the SFRs and/or SARs by completing operations, if these terms are not immediately clear, or are used outside their dictionary definition.

The goal of this work unit is to ensure that the SFRs and SARs are well-defined and that no misunderstanding may occur due to the introduction of vague terms. This work unit should not be taken into extremes, by forcing the PP writer to define every single word. The general audience of a set of security requirements should be assumed to have a reasonable knowledge of IT, security and “Evaluation criteria for IT security”.

All of the above may be presented in groups, classes, roles, types or other groupings or characterisations that allow easy understanding.

The evaluator is reminded that these lists and definitions do not have to be part of the statement of security requirements, but may be placed (in part or in whole) in different subclauses. This may be especially applicable if the same terms are used in the rest of the PP.

ISO/IEC 15408-3 APE_REQ.2.3C: *The statement of security requirements shall identify all operations on the security requirements.*

8.8.2.3.4 Work unit APE_REQ.2-4

The evaluator **shall check** that the statement of security requirements identifies all operations on the security requirements.

The evaluator determines that all operations are identified in each SFR or SAR where such an operation is used. This includes both completed operations and uncompleted operations. Identification may be achieved by typographical distinctions, or by explicit identification in the surrounding text, or by any other distinctive means.

ISO/IEC 15408-3 APE_REQ.2.4C: *All operations shall be performed correctly.*

8.8.2.3.5 Work unit APE_REQ.2-5

The evaluator **shall examine** the statement of security requirements to determine that all assignment operations are performed correctly.

Guidance on the correct performance of operations may be found in ISO/IEC 15408-1 Annex C, Guidance for Operations.