

DIN EN ISO/IEC 18045



ICS 35.030

Entwurf

Einsprüche bis 2024-01-17
Vorgesehen als Ersatz für
DIN EN ISO/IEC 18045:2021-02

**Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre –
Evaluationskriterien für IT-Sicherheit –
Methodik für die Bewertung der IT-Sicherheit (ISO/IEC 18045:2022);
Deutsche und Englische Fassung prEN ISO/IEC 18045:2023**

Information security, cybersecurity and privacy protection –
Evaluation criteria for IT security –
Methodology for IT security evaluation (ISO/IEC 18045:2022);
German and English version prEN ISO/IEC 18045:2023

Sécurité de l'information, cybersécurité et protection de la vie privée –
Critères d'évaluation pour la sécurité des technologies de l'information –
Méthodologie pour l'évaluation de sécurité (ISO/IEC 18045:2022);
Version allemande et anglaise prEN ISO/IEC 18045:2023

Anwendungswarnvermerk

Dieser Entwurf mit Erscheinungsdatum 2023-11-17 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil das beabsichtigte Dokument 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 oder Am DIN-Platz, Burggrafenstr. 6, 10787 Berlin.

Es wird gebeten, mit den Kommentaren zu diesem Entwurf jegliche relevanten Patentrechte, die bekannt sind, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 929 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

Nationales Vorwort

Der Text von ISO/IEC 18045:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 18045:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

Das zuständige nationale Normungsgremium ist der Gemeinschaftsarbeitsausschuss NA 043-04-13 GA „DIN/DKE Gemeinschaftsgremium Cybersecurity“ im DIN-Normenausschuss Informationstechnik und Anwendungen (NIA).

Um Zweifelsfälle in der Übersetzung auszuschließen, ist die englische Originalfassung beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen Text.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Änderungen

Gegenüber DIN EN ISO/IEC 18045:2021-02 wurden folgende Änderungen vorgenommen:

- a) exakter Konformitätstyp eingeführt;
- b) PPs mit geringer Sicherheit entfernt und PPs mit direkter Begründung eingeführt;
- c) PP-Module und PP-Konfigurationen für modulare Evaluationen eingeführt;
- d) Bewertung mit mehreren Sicherheiten eingeführt;
- e) redaktionelle Überarbeitung des Dokuments.

<i>Titel de:</i>	Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre — Evaluationskriterien für IT-Sicherheit — Methodik für die Bewertung der IT-Sicherheit (ISO/IEC 18045:2022)
<i>Titel en:</i>	Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Methodology for IT security evaluation (ISO/IEC 18045:2022)
<i>Titel fr:</i>	Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information — Méthodologie pour l'évaluation de sécurité (ISO/IEC 18045:2022)

Inhalt

	Seite
Europäisches Vorwort	8
Vorwort	9
Rechtliche Hinweise	10
Einleitung	11
1 Anwendungsbereich	12
2 Normative Verweisungen	12
3 Begriffe	12
4 Symbole und Abkürzungen	15
5 Terminologie	15
6 Verbgebrauch	15
7 Allgemeine Evaluierungsleitlinien	16
8 Beziehung zwischen der Normenreihe ISO/IEC 15408 und den Strukturen von ISO/IEC 18045	16
9 Evaluierungsprozess und damit verbundene Arbeitsaufgaben	17
9.1 Allgemein	17
9.2 Überblick über den Evaluierungsprozess	17
9.2.1 Zielsetzungen	17
9.2.2 Verantwortlichkeiten der Rollen	17
9.2.3 Beziehung der Rollen	18
9.2.4 Allgemeines Evaluierungsmodell	18
9.2.5 Evaluatoren-Entscheidungen	19
9.3 Eingabearbeitsaufgabe der Evaluierung	21
9.3.1 Zielsetzungen	21
9.3.2 Anwendungshinweise	21
9.3.3 Management der Teilarbeitsaufgabe der Evaluationsnachweise	22
9.4 Evaluierungsunteraufgaben	23
9.5 Ausgabearbeitsaufgabe der Evaluierung	23
9.5.1 Zielsetzungen	23
9.5.2 Management der Evaluierungsausgaben	23
9.5.3 Anwendungshinweise	23
9.5.4 OR-Teilarbeitsaufgabe schreiben	23
9.5.5 ETR-Teilarbeitsaufgabe schreiben	24
10 Klasse APE: Evaluierung des Schutzprofils	32
10.1 Allgemeines	32
10.2 Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs	33
10.3 PP-Einleitung (APE_INT)	33
10.3.1 Evaluierung der Unteraufgabe (APE_INT.1)	33
10.4 Konformitätsansprüche (APE_CCL)	35
10.4.1 Evaluierung der Unteraufgabe (APE_CCL.1)	35
10.5 Sicherheitsproblemdefinition (APE_SPD)	45
10.5.1 Evaluierung der Unteraufgabe (APE_SPD.1)	45
10.6 Sicherheitszielsetzungen (APE_OBJ)	47

10.6.1	Evaluierung der Unteraufgabe (APE_OBJ.1)	47
10.6.2	Evaluierung der Unteraufgabe (APE_OBJ.2)	48
10.7	Erweiterte Komponentendefinition (APE_ECD)	51
10.7.1	Evaluierung der Unteraufgabe (APE_ECD.1)	51
10.8	Sicherheitsanforderungen (APE_REQ)	55
10.8.1	Evaluierung der Unteraufgabe (APE_REQ.1)	55
10.8.2	Evaluierung der Unteraufgabe (APE_REQ.2)	61
11	Klasse ACE: Evaluierung der Schutzprofilkonfiguration	66
11.1	Allgemeines	66
11.2	Einleitung für PP-Module (ACE_INT)	68
11.2.1	Evaluierung der Unteraufgabe (ACE_INT.1)	68
11.3	Konformitätsansprüche des PP-Moduls (ACE_CCL)	70
11.3.1	Evaluierung der Unteraufgabe (ACE_CCL.1)	70
11.4	Sicherheitsproblemdefinition des PP-Moduls (ACE_SPD)	76
11.4.1	Evaluierung der Unteraufgabe (ACE_SPD.1)	76
11.5	Sicherheitszielsetzungen des PP-Moduls (ACE_OBJ)	77
11.5.1	Evaluierung der Unteraufgabe (ACE_OBJ.1)	77
11.5.2	Evaluierung der Unteraufgabe (ACE_OBJ.2)	78
11.6	Erweiterte Komponentendefinition des PP-Moduls (ACE_ECD)	81
11.6.1	Evaluierung der Unteraufgabe (ACE_ECD.1)	81
11.7	Sicherheitsanforderungen des PP-Moduls (ACE_REQ)	85
11.7.1	Evaluierung der Unteraufgabe (ACE_REQ.1)	85
11.7.2	Evaluierung der Unteraufgabe (ACE_REQ.2)	91
11.8	Konsistenz des PP-Moduls (ACE_MCO)	97
11.8.1	Evaluierung der Unteraufgabe (ACE_MCO.1)	97
11.9	Konsistenz der PP-Konfiguration (ACE_CCO)	100
11.9.1	Evaluierung der Unteraufgabe (ACE_CCO.1)	100
12	Klasse ASE: Evaluierung der Sicherheitsvorgabe	109
12.1	Allgemeines	109
12.2	Anwendungshinweise	109
12.2.1	Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs	109
12.3	ST-Einleitung (ASE_INT)	110
12.3.1	Evaluierung der Unteraufgabe (ASE_INT.1)	110
12.4	Konformitätsansprüche (ASE_CCL)	114
12.4.1	Evaluierung der Unteraufgabe (ASE_CCL.1)	114
12.5	Sicherheitsproblemdefinition (ASE_SPD)	129
12.5.1	Evaluierung der Unteraufgabe (ASE_SPD.1)	129
12.6	Sicherheitszielsetzungen (ASE_OBJ)	131
12.6.1	Evaluierung der Unteraufgabe (ASE_OBJ.1)	131
12.6.2	Evaluierung der Unteraufgabe (ASE_OBJ.2)	132
12.7	Erweiterte Komponentendefinition (ASE_ECD)	135
12.7.1	Evaluierung der Unteraufgabe (ASE_ECD.1)	135
12.8	Sicherheitsanforderungen (ASE_REQ)	139
12.8.1	Evaluierung der Unteraufgabe (ASE_REQ.1)	139
12.8.2	Evaluierung der Unteraufgabe (ASE_REQ.2)	145
12.9	Zusammenfassende Spezifikation des TOE (ASE_TSS)	152
12.9.1	Evaluierung der Unteraufgabe (ASE_TSS.1)	152
12.9.2	Evaluierung der Unteraufgabe (ASE_TSS.2)	153
12.10	Konsistenz der Sicherheitsvorgaben des Verbundprodukts (ASE_COMP)	154
12.10.1	Allgemeines	154
12.10.2	Evaluierung der Unteraufgabe (ASE_COMP.1)	155
13	Klasse ADV: Entwicklung	160
13.1	Allgemeines	160
13.2	Anwendungshinweise	161

13.3	Sicherheitsarchitektur (ADV_ARC)	161
13.3.1	Evaluierung der Unteraufgabe (ADV_ARC.1).....	161
13.4	Funktionsspezifikation (ADV_FSP)	167
13.4.1	Evaluierung der Unteraufgabe (ADV_FSP.1).....	167
13.4.2	Evaluierung der Unteraufgabe (ADV_FSP.2).....	171
13.4.3	Evaluierung der Unteraufgabe (ADV_FSP.3).....	176
13.4.4	Evaluierung der Unteraufgabe (ADV_FSP.4).....	182
13.4.5	Evaluierung der Unteraufgabe (ADV_FSP.5).....	188
13.4.6	Evaluierung der Unteraufgabe (ADV_FSP.6).....	195
13.5	Darstellung der Implementierung (ADV_IMP).....	195
13.5.1	Evaluierung der Unteraufgabe (ADV_IMP.1).....	195
13.5.2	Evaluierung der Unteraufgabe (ADV_IMP.2).....	197
13.6	TSF-Interna (ADV_INT)	201
13.6.1	Evaluierung der Unteraufgabe (ADV_INT.1).....	201
13.6.2	Evaluierung der Unteraufgabe (ADV_INT.2).....	203
13.6.3	Evaluierung der Unteraufgabe (ADV_INT.3).....	206
13.7	Formales TSF-Modell (ADV_SPM)	209
13.7.1	Evaluierung der Unteraufgabe (ADV_SPM.1)	209
13.8	TOE-Design (ADV_TDS).....	216
13.8.1	Evaluierung der Unteraufgabe (ADV_TDS.1).....	216
13.8.2	Evaluierung der Unteraufgabe (ADV_TDS.2).....	220
13.8.3	Evaluierung der Unteraufgabe (ADV_TDS.3).....	226
13.8.4	Evaluierung der Unteraufgabe (ADV_TDS.4).....	236
13.8.5	Evaluierung der Unteraufgabe (ADV_TDS.5).....	246
13.8.6	Evaluierung der Unteraufgabe (ADV_TDS.6).....	255
13.9	Konformität mit dem zusammengesetzten Design (ADV_COMP)	256
13.9.1	Allgemeines	256
13.9.2	Evaluierung der Unteraufgabe (ADV_COMP.1)	256
14	Klasse AGD: Leitliniendokumente.....	258
14.1	Allgemeines	258
14.2	Anwendungshinweise.....	258
14.3	Operative Leitlinien für Benutzer (AGD_OPE)	259
14.3.1	Evaluierung der Unteraufgabe (AGD_OPE.1).....	259
14.4	Vorbereitende Verfahren (AGD_PRE)	262
14.4.1	Evaluierung der Unteraufgabe (AGD_PRE.1).....	262
15	Klasse ALC: Unterstützung des Lebenszyklus	264
15.1	Allgemeines	264
15.2	CM-Funktionen (ALC_CMC).....	265
15.2.1	Evaluierung der Unteraufgabe (ALC_CMC.1)	265
15.2.2	Evaluierung der Unteraufgabe (ALC_CMC.2)	266
15.2.3	Evaluierung der Unteraufgabe (ALC_CMC.3)	268
15.2.4	Evaluierung der Unteraufgabe (ALC_CMC.4)	272
15.2.5	Evaluierung der Unteraufgabe (ALC_CMC.5)	278
15.3	CM-Umfang (ALC_CMS).....	286
15.3.1	Evaluierung der Unteraufgabe (ALC_CMS.1)	286
15.3.2	Evaluierung der Unteraufgabe (ALC_CMS.2)	287
15.3.3	Evaluierung der Unteraufgabe (ALC_CMS.3)	288
15.3.4	Evaluierung der Unteraufgabe (ALC_CMS.4)	289
15.3.5	Evaluierung der Unteraufgabe (ALC_CMS.5)	290
15.4	Lieferung (ALC_DEL)	292
15.4.1	Evaluierung der Unteraufgabe (ALC_DEL.1).....	292
15.5	Entwicklungssicherheit (ALC_DVS).....	293
15.5.1	Evaluierung der Unteraufgabe (ALC_DVS.1).....	293
15.5.2	Evaluierung der Unteraufgabe (ALC_DVS.2).....	296

15.6	Mängelbeseitigung (ALC_FLR)	299
15.6.1	Evaluierung der Unteraufgabe (ALC_FLR.1)	299
15.6.2	Evaluierung der Unteraufgabe (ALC_FLR.2)	302
15.6.3	Evaluierung der Unteraufgabe (ALC_FLR.3)	306
15.7	Definition des Lebenszyklus (ALC_LCD)	312
15.7.1	Evaluierung der Unteraufgabe (ALC_LCD.1)	312
15.7.2	Evaluierung der Unteraufgabe (ALC_LCD.2)	313
15.8	Artefakte der TOE-Entwicklung (ALC_TDA)	315
15.8.1	Evaluierung der Unteraufgabe (ALC_TDA.1)	315
15.8.2	Evaluierung der Unteraufgabe (ALC_TDA.2)	319
15.8.3	Evaluierung der Unteraufgabe (ALC_TDA.3)	322
15.9	Tools und Techniken (ALC_TAT)	327
15.9.1	Evaluierung der Unteraufgabe (ALC_TAT.1)	327
15.9.2	Evaluierung der Unteraufgabe (ALC_TAT.2)	329
15.9.3	Evaluierung der Unteraufgabe (ALC_TAT.3)	332
15.10	Integration von Zusammensetzungsteilen und Konsistenzprüfung von Lieferverfahren (ALC_COMP)	336
15.10.1	Allgemeines	336
15.10.2	Evaluierung der Unteraufgabe (ALC_COMP.1)	336
16	Klasse ATE: Prüfungen	339
16.1	Allgemeines	339
16.2	Anwendungshinweise	339
16.2.1	Verständnis des erwarteten Verhaltens des TOE	340
16.2.2	Prüfen gegenüber alternativen Ansätzen zur Überprüfung des erwarteten Verhaltens der Funktionalität	340
16.2.3	Überprüfung der Angemessenheit der Prüfungen	340
16.3	Abdeckung (ATE_COV)	341
16.3.1	Evaluierung der Unteraufgabe (ATE_COV.1)	341
16.3.2	Evaluierung der Unteraufgabe (ATE_COV.2)	342
16.3.3	Evaluierung der Unteraufgabe (ATE_COV.3)	343
16.4	Tiefe (ATE_DPT)	345
16.4.1	Evaluierung der Unteraufgabe (ATE_DPT.1)	345
16.4.2	Evaluierung der Unteraufgabe (ATE_DPT.2)	348
16.4.3	Evaluierung der Unteraufgabe (ATE_DPT.3)	351
16.4.4	Evaluierung der Unteraufgabe (ATE_DPT.4)	354
16.5	Funktionsprüfungen (ATE_FUN)	354
16.5.1	Evaluierung der Unteraufgabe (ATE_FUN.1)	354
16.5.2	Evaluierung der Unteraufgabe (ATE_FUN.2)	357
16.6	Unabhängiges Prüfen (ATE_IND)	362
16.6.1	Evaluierung der Unteraufgabe (ATE_IND.1)	362
16.6.2	Evaluierung der Unteraufgabe (ATE_IND.2)	366
16.6.3	Evaluierung der Unteraufgabe (ATE_IND.3)	372
16.7	Zusammengesetzte Funktionsprüfung (ATE_COMP)	372
16.7.1	Allgemeines	372
16.7.2	Evaluierung der Unteraufgabe (ATE_COMP.1)	372
17	Klasse AVA: Anfälligkeitsbewertung	374
17.1	Allgemeines	374
17.2	Anfälligkeitsanalyse (AVA_VAN)	374
17.2.1	Evaluierung der Unteraufgabe (AVA_VAN.1)	374
17.2.2	Evaluierung der Unteraufgabe (AVA_VAN.2)	380
17.2.3	Evaluierung der Unteraufgabe (AVA_VAN.3)	387
17.2.4	Evaluierung der Unteraufgabe (AVA_VAN.4)	397
17.2.5	Evaluierung der Unteraufgabe (AVA_VAN.5)	405
17.3	Zusammengesetzte Anfälligkeitsbewertung (AVA_COMP)	413

17.3.1	Allgemeines	413
17.3.2	Evaluierung der Unteraufgabe (AVA_COMP.1)	413
18	Klasse ACO: Zusammensetzung.....	416
18.1	Allgemeines	416
18.2	Anwendungshinweise	416
18.3	Begründung der Zusammensetzung (ACO_COR).....	417
18.3.1	Evaluierung der Unteraufgabe (ACO_COR.1)	417
18.4	Entwicklungsnachweis (ACO_DEV)	424
18.4.1	Evaluierung der Unteraufgabe (ACO_DEV.1).....	424
18.4.2	Evaluierung der Unteraufgabe (ACO_DEV.2).....	425
18.4.3	Evaluierung der Unteraufgabe (ACO_DEV.3).....	427
18.5	Verlässlichkeit der abhängigen Komponente (ACO_REL)	430
18.5.1	Evaluierung der Unteraufgabe (ACO_REL.1)	430
18.5.2	Evaluierung der Unteraufgabe (ACO_REL.2)	432
18.6	Prüfen des zusammengesetzten TOE (ACO_CTT).....	435
18.6.1	Evaluierung der Unteraufgabe (ACO_CTT.1)	435
18.6.2	Evaluierung der Unteraufgabe (ACO_CTT.2)	438
18.7	Anfälligkeitsanalyse der Zusammensetzung (ACO_VUL).....	441
18.7.1	Evaluierung der Unteraufgabe (ACO_VUL.1)	441
18.7.2	Anwendungshinweise	442
18.7.3	Evaluierung der Unteraufgabe (ACO_VUL.2)	445
18.7.4	Evaluierung der Unteraufgabe (ACO_VUL.3)	449
Anhang A (informativ)	Allgemeine Evaluierungsleitlinien.....	453
A.1	Zielsetzungen	453
A.2	Probenahme	453
A.3	Abhängigkeiten	455
A.3.1	Allgemeines	455
A.3.2	Abhängigkeiten zwischen Aufgaben.....	455
A.3.3	Abhängigkeiten zwischen Unteraufgaben.....	455
A.3.4	Abhängigkeiten zwischen Aktionen	456
A.4	Ortsbegehungen.....	456
A.4.1	Allgemeines	456
A.4.2	Allgemeiner Ansatz.....	457
A.5	Orientierungshilfe für die Erstellung der Checkliste	457
A.5.1	Aspekte des Konfigurationsmanagements	458
A.5.2	Aspekte der Entwicklungssicherheit.....	458
A.5.3	Beispiel für eine Checkliste.....	459
A.6	Zuständigkeiten des Systems	461
Anhang B (informativ)	Anfälligkeitsbewertung (AVA).....	463
B.1	Was bedeutet Anfälligkeitsanalyse.....	463
B.2	Erstellung einer Anfälligkeitsanalyse durch den Evaluator	464
B.3	Allgemeine Leitlinien für Anfälligkeiten.....	464
B.3.1	Umgehen	464
B.3.2	Manipulation	466
B.3.3	Direkte Angriffe.....	469
B.3.4	Überwachung	470
B.3.5	Fehlbenutzung.....	471
B.4	Identifizierung potentieller Anfälligkeiten.....	472
B.4.1	Erkennen	472
B.4.2	Analyse	473
B.5	Bei Verwendung des Angriffspotentials.....	475
B.5.1	Entwickler	475
B.5.2	Evaluator.....	476
B.6	Berechnung des Angriffspotentials.....	477

B.6.1	Anwendung des Angriffspotentials.....	477
B.6.2	Charakterisierung des Angriffspotentials.....	478
B.7	Beispielrechnung für einen direkten Angriff.....	485
Anhang C (informativ) Evaluierungstechniken und -Tools		487
C.1	Semiformale und formale Verfahren	487
C.1.1	Allgemeines	487
C.1.2	Beschreibung der Stile.....	487

Europäisches Vorwort

Der Text von ISO/IEC 18045:2022 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) erarbeitet und als prEN ISO/IEC 18045:2023 durch das Technische Komitee CEN/CLC/JTC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Dieses Dokument ist derzeit zur CEN-Umfrage vorgelegt.

Dieses Dokument wird EN ISO/IEC 18045:2020 ersetzen.

Anerkennungsnotiz

Der Text von ISO/IEC 18045:2022 wurde von CEN als prEN ISO/IEC 18045:2023 ohne irgendeine Abänderung genehmigt.

Vorwort

ISO (die Internationale Organisation für Normung) und IEC (die Internationale Elektrotechnische Kommission) bilden das auf die weltweite Normung spezialisierte System. Nationale Normungsorganisationen, die Mitglieder von ISO oder IEC sind, beteiligen sich an der Entwicklung von Internationalen Normen in Technischen Komitees, die von der jeweiligen Organisation eingerichtet wurden, um spezifische Gebiete technischer Aktivitäten zu behandeln. Auf Gebieten von beiderseitigem Interesse arbeiten die Technischen Komitees von ISO und IEC zusammen. Weitere internationale staatliche und nichtstaatliche Organisationen, die in engem Kontakt mit ISO und IEC stehen, nehmen ebenfalls an der Arbeit teil.

Die Verfahren, die bei der Entwicklung dieses Dokuments angewendet wurden und die für die weitere Pflege vorgesehen sind, werden in den ISO/IEC-Directives, Teil 1 beschrieben. Im Besonderen sollten die für die verschiedenen ISO-Dokumentenarten notwendigen Annahmekriterien beachtet werden. Dieses Dokument wurde in Übereinstimmung mit den Gestaltungsregeln der ISO/IEC-Directives, Teil 2 erarbeitet (siehe www.iso.org/directives oder www.iec.ch/members_experts/refdocs).

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. ISO und IEC sind nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren. Details zu allen während der Entwicklung des Dokuments identifizierten Patentrechten finden sich in der Einleitung und/oder in der ISO-Liste der erhaltenen Patenterklärungen (siehe www.iso.org/patents) oder in der IEC-Liste der erhaltenen Patenterklärungen (siehe <http://patents.iec.ch>).

Jeder in diesem Dokument verwendete Handelsname dient nur zur Unterrichtung der Anwender und bedeutet keine Anerkennung.

Für eine Erläuterung des freiwilligen Charakters von Normen, der Bedeutung ISO-spezifischer Begriffe und Ausdrücke in Bezug auf Konformitätsbewertungen sowie Informationen darüber, wie ISO die Grundsätze der Welthandelsorganisation (WTO, en: World Trade Organization) hinsichtlich technischer Handelshemmnisse (TBT, en: Technical Barriers to Trade) berücksichtigt, siehe www.iso.org/iso/foreword.html. In der IEC, siehe www.iec.ch/understanding-standards.

Dieses Dokument wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *Information security, cybersecurity and privacy protection*, erarbeitet.

Diese dritte Ausgabe ersetzt die zweite Ausgabe (ISO/IEC 18045:2008), die technisch überarbeitet wurde.

Die wesentlichen Änderungen sind folgende:

- der genaue Konformitätstyp wurde eingeführt;
- die PP mit niedriger Vertrauenswürdigkeit wurden entfernt und die PP mit direkter Begründung eingeführt;
- PP-Module und PP-Konfigurationen für modulare Evaluierungen wurden eingeführt;
- eine Evaluierung mit Mehrfach-Vertrauenswürdigkeit wurde eingeführt.

Rückmeldungen oder Fragen zu diesem Dokument sollten an das jeweilige nationale Normungsinstitut des Anwenders gerichtet werden. Eine vollständige Auflistung dieser Institute ist unter www.iso.org/members.html und www.iec.ch/national-committees zu finden.

Rechtliche Hinweise

Die nachfolgend aufgeführten Regierungsorganisationen haben an der Entwicklung dieser Version der Gemeinsamen Methodik für die Bewertungen der IT-Sicherheit mitgewirkt. Als gemeinsame Inhaber des Urheberrechts an der Gemeinsamen Methodik für Bewertungen der IT-Sicherheit (genannt CEM), gewähren sie der ISO/IEC hiermit eine nicht-exklusive Lizenz zur Nutzung von CEM bei der Weiterentwicklung/Pflege der Internationalen Norm ISO/IEC 18045. Diese Regierungsorganisationen behalten jedoch das Recht, CEM nach eigenem Ermessen zu nutzen, zu kopieren, zu verteilen, zu übersetzen oder zu modifizieren.

Australien	Australian Signals Directorate
Kanada	Communications Security Establishment
Frankreich	Agence Nationale de la Sécurité des Systèmes d'Information
Deutschland	Bundesamt für Sicherheit in der Informationstechnik
Japan	Information-technology Promotion Agency
Niederlande	Netherlands National Communications Security Agency
Neuseeland	Government Communications Security Bureau
Republik Korea	National Security Research Institute
Spanien	Ministerio de Asuntos Económicos y Transformación Digital
Schweden	FMV, Swedish Defence Materiel Administration
Vereinigtes Königreich	National Cyber Security Centre
Vereinigte Staaten	National Security Agency

Einleitung

Die Zielgruppe für dieses Dokument sind in erster Linie Evaluatoren, die die Normenreihe ISO/IEC 15408 anwenden, und Zertifizierer, die die Evaluatorenaktionen bestätigen; Antragsteller der Evaluierung, Entwickler, Schutzprofil (PP), PP-Modul, PP-Konfiguration sowie Autoren der Sicherheitsvorgabe (ST) und andere an der IT-Sicherheit interessierte Parteien können eine sekundäre Zielgruppe sein.

Dieses Dokument kann nicht alle Fragen zur Evaluierung der IT-Sicherheit beantworten, so dass möglicherweise weitere Interpretationen notwendig sind. Einzelne Schemata legen fest, wie mit solchen Interpretationen umzugehen ist, auch wenn diese Gegenstand von Vereinbarungen über die gegenseitige Anerkennung sein können. Eine Liste der methodenbezogenen Aufgaben, die im Rahmen der einzelnen Schemata durchgeführt werden können, findet sich in Anhang A.

Dieses Dokument ist für die Anwendung in Verbindung mit der Normenreihe ISO/IEC 15408 vorgesehen.

ANMERKUNG 1 Die Verweisung in diesem Dokument auf ISO/IEC 15408 bezieht sich auf die Normenreihe ISO/IEC 15408.

ANMERKUNG 2 Im vorliegenden Dokument werden einige Begriffe fett und kursiv gedruckt, um sie vom übrigen Text abzuheben. Die Beziehung zwischen den Komponenten einer Familie wird als Konvention über eine Fettmarkierung hervorgehoben. Diese Markierungskonvention erfordert die Verwendung von Fettdruck für alle neuen Anforderungen. Für hierarchische Komponenten werden Anforderungen fett hervorgehoben, wenn sie über die Anforderungen der vorherigen Komponente hinaus erweitert oder geändert werden. Zusätzlich werden alle neuen oder erweiterten zulässigen über die vorherige Komponente hinausgehenden Operationen auch fett hervorgehoben.

Die Verwendung von Kursivschrift weist auf einen Text hin, der eine genaue Bedeutung hat. Für die Vertrauenswürdigkeitsanforderungen gilt die Konvention für spezielle Verben, die sich auf die Evaluierung beziehen.

1 Anwendungsbereich

Dieses Dokument legt die Aktionen fest, die ein Evaluator mindestens durchführen muss, um eine Evaluierung nach der Normenreihe ISO/IEC 15408 unter Verwendung der in der Normenreihe ISO/IEC 15408 definierten Kriterien und Evaluationsnachweise durchzuführen.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

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

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

ISO/IEC 15408-3:2022, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 15408-4, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*

ISO/IEC 15408-5, *Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*

ISO/IEC IEEE 24765, *Systems and software engineering — Vocabulary*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3, ISO/IEC 15408-4, ISO/IEC 15408-5, ISO/IEC IEEE 24765 und die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

— IEC Electropedia: verfügbar unter <https://www.electropedia.org/>

— ISO Online Browsing Platform: verfügbar unter <https://www.iso.org/obp>

3.1

prüfen, Verb

<Evaluierung> auf Grundlage eines einfachen Vergleichs eine Entscheidung treffen

Anmerkung 1 zum Begriff: Fachwissen eines Evaluatoren ist nicht erforderlich. Eine Aussage, die dieses Verb verwendet, beschreibt eine Zuordnung.

3.2

bestätigen, Verb

<Evaluierung> erklären, dass etwas detailliert und mit einer unabhängig bestimmten Angemessenheit geprüft wurde

Anmerkung 1 zum Begriff: Die erforderliche Stufe der Stringenz hängt von der Art des Gegenstands ab.

3.3

nachweisen, Verb

<Evaluierung> durch eine Analyse gewonnene Schlussfolgerung liefern, die weniger stringent ist als ein „Beweis“

3.4

beschreiben, Verb

<Evaluierung> spezifische Angaben zu einer Entität bereitstellen

3.5

bestimmen, Verb

<Evaluierung> bestimmte Schlussfolgerung auf Basis einer unabhängigen Analyse bestätigen mit dem Ziel, eine bestimmte Schlussfolgerung zu erreichen

Anmerkung 1 zum Begriff: Die Verwendung dieses Begriffs setzt eine wirklich unabhängige Analyse voraus, in der Regel ohne dass eine vorhergehende Analyse durchgeführt wurde. Vergleich mit den Begriffen „bestätigen“ (3.2) oder „verifizieren“, die voraussetzen, dass bereits eine Analyse durchgeführt wurde, die es zu überprüfen gilt.

3.6

aufgedeckte mögliche Anfälligkeit

potentielle Schwachstellen in den Evaluationsgegenständen (TOE), die vom Evaluator bei der Durchführung von Evaluierungsaufgaben festgestellt werden und die zur Verletzung der Sicherheitsfunktionsanforderungen (SFR) genutzt werden können

3.7

sicherstellen, Verb

<Evaluierung> engen Kausalzusammenhang zwischen einer Aktion und ihren Folgen garantieren

Anmerkung 1 zum Begriff: Wenn dem Wort „sicherstellen“ das Wort „helfen“ vorangestellt ist, bedeutet dies, dass die Folge allein aufgrund dieser Aktion nicht völlig sicher ist.

3.8

Evaluationsnachweis

Element, das als Grundlage für die Erstellung der Entscheidung über eine Evaluierungsaufgabe verwendet wird

3.9

untersuchen, Verb

<Evaluierung> mittels Analyse und unter Nutzung von Evaluatoren-Fachwissen eine Entscheidung treffen

Anmerkung 1 zum Begriff: Eine Aussage, die dieses Verb verwendet, nennt die analysierten Sachverhalte und die Eigenschaften, aufgrund derer die Analyse durchgeführt wurde.

3.10

erschöpfend, Adjektiv

<Evaluierung> Merkmal eines methodischen Ansatzes zur Durchführung einer Analyse oder Aufgabe nach einem eindeutigen Plan

Anmerkung 1 zum Begriff: Dieser Begriff wird in den entsprechenden Teilen der Normenreihe ISO/IEC 15408 in Bezug auf die Durchführung einer Analyse oder einer anderen Aufgabe verwendet. Er steht in Zusammenhang mit „systematisch“, ist aber wesentlich stärker, da er nicht nur darauf hinweist, dass ein methodischer Ansatz gewählt wurde, um die Analyse oder Aufgabe nach einem eindeutigen Plan durchzuführen, sondern auch darauf, dass der verfolgte Plan ausreicht, um *sicherzustellen* (3.7), dass alle möglichen Wege ausgeschöpft wurden.

3.11

erklären, Verb

<Evaluierung> argumentative Darlegung des Grundes für eine bestimmte Vorgehensweise

Anmerkung 1 zum Begriff: Dieser Begriff unterscheidet sich sowohl von „*beschreiben*“ (3.4) als auch von „*nachweisen*“ (3.3). Damit soll die Frage „Warum?“ beantwortet werden, ohne dabei behaupten zu wollen, dass die gewählte Vorgehensweise zwangsläufig optimal war.

3.12

begründen, Verb

<Evaluierung> durch Argumente gestützte Begründung liefern

Anmerkung 1 zum Begriff: Der Begriff „begründen“ ist stringenter als „*nachweisen*“ (3.3). Dieser Begriff erfordert ein hohes Maß an Stringenz, da jeder Schritt einer logischen Analyse, die zu einer Schlussfolgerung führt, sehr vorsichtig und gründlich *erklärt* (3.11) werden muss.

3.13

Überwachungsangriff

generische Kategorie von Angriffsverfahren, einschließlich passiver Analysetechniken, die auf die Offenlegung sensibler interner Daten des Evaluationsgegenstandes (TOE) abzielen, indem der TOE in einer Weise betrieben wird, die den Leitliniendokumenten entspricht

3.14

Beobachtungsbericht

OR, en: observation report

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

3.15

Überwachungsentscheidung

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

3.16

beweisen, Verb

<Evaluierung> Übereinstimmung durch formale Analyse im mathematischen Sinne aufzeigen

Anmerkung 1 zum Begriff: Sie ist in jeder Hinsicht völlig stringent. Üblicherweise wird der Begriff „beweisen“ verwendet, wenn der Wunsch besteht, die Übereinstimmung zwischen zwei Darstellungen der vom Evaluationsgegenstand (TOE) vorgegebenen Sicherheitsfunktionalität (TSF) auf einer hohen Stringenzstufe nachzuweisen.

3.17

aufzeichnen, Verb

<Evaluierung> 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

3.18

berichten, Verb

<Evaluierung> Evaluierungsergebnisse und dokumentierende Angaben und Unterlagen im technischen Evaluierungsbericht, einem *Beobachtungsbericht* (3.14) oder einem Evaluierungsbericht (Bericht der Evaluierungsinstanz) zusammenstellen

3.19

spezifizieren, Verb

<Evaluierung> spezifische Details über eine Entität in einer stringenten und präzisen Weise bereitstellen

3.20

verfolgen, Verb

<Evaluierung> Beziehung zwischen zwei Sätzen von Entitäten herstellen, die zeigt, welche Entitäten des ersten Satzes welchen Entitäten des zweiten Satzes entsprechen

3.21

Entscheidung

Urteil, das ein Evaluator hinsichtlich eines Evaluatorenaktionselements oder einer Vertrauenswürdigkeitskomponente oder -klasse fällt

3.22

verifizieren, Verb

<Evaluierung> stringent, detailliert und mit einer unabhängig bestimmten Angemessenheit prüfen

Anmerkung 1 zum Begriff: Siehe auch „bestätigen“ (3.2). Dieser Begriff hat eine stringenter Bedeutung. Der Begriff „verifizieren“ wird im Zusammenhang mit Evaluatorenaktionen verwendet, wenn eine unabhängige Anstrengung durch den Evaluator erforderlich ist.

3.23

Zugriffsgelegenheit

Zeitspanne, in der ein Angreifer Zugriff auf einen Evaluationsgegenstand (TOE) hat

3.24

Workunit

Ebene der kleinsten Einheiten bei der Durchführung der Evaluierung

4 Symbole und Abkürzungen

OR Beobachtungsbericht (en: observation report)

5 Terminologie

Im Gegensatz zur Normenreihe ISO/IEC 15408, bei der jedes Element die letzte Stelle seines Identifizierungssymbols für alle Komponenten innerhalb der Familie beibehält, kann dieses Dokument neue Workunits einführen, wenn ein Evaluatorenaktionselement der Normenreihe ISO/IEC 15408 von Unteraufgabe zu Unteraufgabe wechselt. Infolgedessen kann sich die letzte Stelle des Erkennungszeichens der Workunit ändern, obwohl die Workunit unverändert bleibt.

Jede erforderliche methodenspezifische Durchführung der Evaluierung, die nicht direkt aus einer Anforderung der Normenreihe ISO/IEC 15408 abgeleitet ist, wird als *Arbeitsaufgabe* oder *Teilarbeitsaufgabe* bezeichnet.

6 Verbgebrauch

Allen Verben der Workunits und der Teilarbeitsaufgaben wird das Hilfsverb *muss* vorangestellt, wobei sowohl das Verb als auch *muss* in ***kursiver Fettschrift*** dargestellt werden. Das Hilfsverb *muss* wird nur verwendet, wenn der vorgegebene Text obligatorisch ist, also nur innerhalb der Workunits und Teilarbeitsaufgaben. Die Workunits und Teilarbeitsaufgaben enthalten obligatorische Aufgaben, die der Evaluator durchführen muss, um Entscheidungen zu treffen.

Die Leitlinien, die mit den Workunits und Teilarbeitsaufgaben einhergehen, geben weitere Erläuterungen zur Anwendung von Wörtern aus ISO/IEC 15408 in einer Evaluierung. Der Verbgebrauch erfolgt in Übereinstimmung mit ISO-Definitionen für diese Verben. Das Hilfsverb *sollte* wird verwendet, um eine Empfehlung auszusprechen. *Darf/dürfen* zeigt eine Zulässigkeit an und *kann/können* eine Möglichkeit.

Die Verben *prüfen*, *untersuchen*, *berichten* und *aufzeichnen* werden mit einer genauen Bedeutung innerhalb dieses Teils dieses Dokuments verwendet, und Abschnitt 3 sollte für deren Definitionen herangezogen werden.

7 Allgemeine Evaluierungsleitlinien

Material, das auf mehr als eine Unteraufgabe anwendbar ist, wird an einer Stelle erfasst. Leitlinien, deren Anwendbarkeit weit verbreitet ist (über alle Aufgaben und EALs hinweg), wurden in Anhang A erfasst. Leitlinien, die sich auf mehrere Unteraufgaben innerhalb einer einzigen Aufgabe beziehen, wurden in der Einleitung zu dieser Aufgabe bereitgestellt. Beziehen sich Leitlinien nur auf eine einzelne Unteraufgabe, werden sie innerhalb dieser Unteraufgabe dargestellt.

8 Beziehung zwischen der Normenreihe ISO/IEC 15408 und den Strukturen von ISO/IEC 18045

Es gibt direkte Beziehungen zwischen der Struktur von Normenreihe ISO/IEC 15408 (d. h. Klasse, Familie, Komponente und Element) und der Struktur dieses Dokuments. Bild 1 veranschaulicht die Entsprechung zwischen den Konstrukten der Normenreihe ISO/IEC 15408 von Klasse, Familie und Evaluatorenaktions-elementen sowie den Aufgaben, Unteraufgaben und Aktionen der Evaluierungsmethodik. Aus den in der Normenreihe ISO/IEC 15408 genannten Anforderungen an das Entwickleraktionselement und den Inhalt und die Nachweisdarstellung können sich jedoch mehrere Workunits zur Evaluierungsmethodik ergeben.

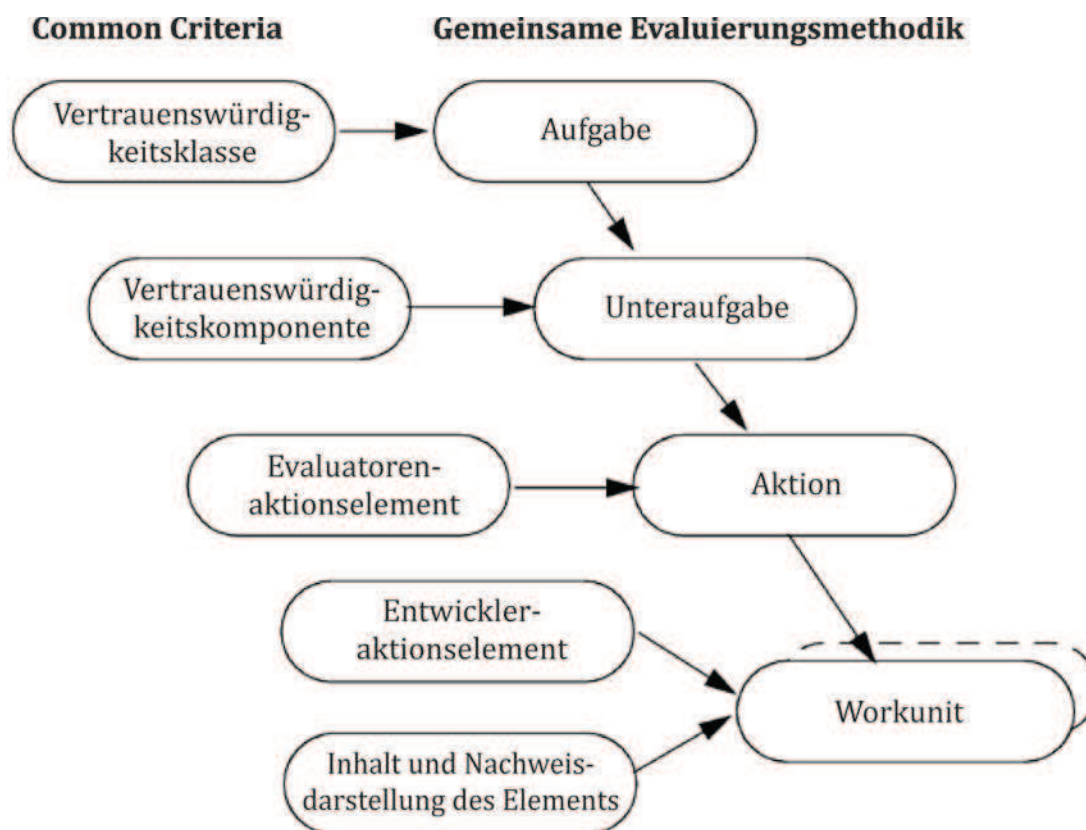


Bild 1 — Zuordnung der Normenreihe ISO/IEC 15408 und den Strukturen von ISO/IEC 18045

9 Evaluierungsprozess und damit verbundene Arbeitsaufgaben

9.1 Allgemein

Dieser Abschnitt gibt einen Überblick über den Evaluierungsprozess und definiert die Aufgaben, die ein Evaluator bei der Durchführung einer Evaluierung durchführen soll.

Jede Evaluierung, ob eines PP, einer PP-Konfiguration oder eines TOE (einschließlich ST), folgt dem gleichen Prozess und hat vier Evaluierungsarbeitsaufgaben gemeinsam: die Eingearbeitsaufgabe, die Ausgabearbeitsaufgabe, die Evaluierungsunteraufgaben und die Vorführung der technischen Kompetenz gegenüber der Arbeitsaufgabe der Evaluierungsinstanz.

Die Eingearbeitsaufgabe und die Ausgabearbeitsaufgaben, die mit dem Management der Evaluationsnachweise und der Berichtserstellung zusammenhängen, werden in diesem Abschnitt vollständig beschrieben. Jede Arbeitsaufgabe hat zugehörige Teilarbeitsaufgaben, die für alle Evaluierungen nach ISO/IEC 15408 (Evaluierung eines PP, einer PP-Konfiguration oder eines TOE) gelten.

Die Evaluierungsunteraufgaben werden in diesem Abschnitt nur angeschnitten und in den folgenden Kapiteln ausführlich beschrieben.

Im Gegensatz zu den Evaluierungsunteraufgaben sind mit den Eingabe- und Ausgabearbeitsaufgaben keine Entscheidungen verbunden, da sie nicht die Evaluatorenaktionselemente nach ISO/IEC 15408 abbilden; sie werden durchgeführt, um die Übereinstimmung mit den universellen Grundsätzen sicherzustellen und mit diesem Dokument konform zu sein.

Die Vorführung der technischen Kompetenz gegenüber der Arbeitsaufgabe der Evaluierungsinstanz kann durch die Analyse der Ausgabeergebnisse der Arbeitsaufgaben der Evaluierungsinstanz erbracht werden, oder es kann die Vorführung enthalten sein, dass die Evaluatoren die Eingaben für die Unteraufgaben der Evaluierung verstanden haben. Mit dieser Arbeitsaufgabe ist keine Evaluator-Entscheidung verbunden, sondern eine Entscheidung der Evaluierungsinstanz. Die detaillierten Kriterien zur Absolvierung dieser Arbeitsaufgabe liegen im Ermessen der Evaluierungsinstanz, wie in Abschnitt A.6 angegeben.

Evaluierungsaufgaben, die in Übereinstimmung mit ISO/IEC 15408-4 festgelegt sind, können anstelle der in diesem Dokument definierten Workunits verwendet werden, sofern dies in den Evaluierungs- und Zertifizierungsberichten deutlich gemacht wird.

9.2 Überblick über den Evaluierungsprozess

9.2.1 Zielsetzungen

Dieser Unterabschnitt stellt das allgemeine Modell der Methodik dar und legt Folgendes fest:

- a) Rollen und Verantwortlichkeiten der in den Evaluierungsprozess einbezogenen Parteien;
- b) das allgemeine Evaluierungsmodell.

9.2.2 Verantwortlichkeiten der Rollen

Das allgemeine Modell legt die folgenden Rollen fest: Antragsteller, Entwickler, Evaluator und Evaluierungsinstanz.

Der Antragsteller ist für die Antragstellung und Unterstützung einer Evaluierung verantwortlich. Dies bedeutet, dass der Antragsteller die verschiedenen Vereinbarungen für die Evaluierung (z. B. die Beauftragung der Evaluierung) trifft. Darüber hinaus ist der Antragsteller dafür verantwortlich, dass dem Evaluator die Evaluationsnachweise zur Verfügung gestellt werden.

Der Entwickler erstellt den TOE und ist dafür verantwortlich, im Auftrag des Antragstellers die für die Evaluierung erforderlichen Nachweise (z. B. Schulung, Designinformationen) zu erbringen.

Der Evaluator führt die im Zusammenhang mit einer Evaluierung erforderlichen Evaluierungsarbeitsaufgaben aus: Der Evaluator erhält die Evaluationsnachweise vom Entwickler im Namen des Antragstellers oder direkt vom Antragsteller, führt die Evaluierungsunteraufgaben durch und stellt die Ergebnisse der Evaluierungsbeurteilung der Evaluierungsinstanz zur Verfügung.

Die Evaluierungsinstanz erstellt und pflegt das Schema, überwacht die vom Evaluator durchgeführte Evaluierung und stellt auf der Grundlage der vom Evaluator gelieferten Evaluierungsergebnisse Zertifizierungs-/Validierungsberichte sowie Zertifikate aus.

9.2.3 Beziehung der Rollen

Um zu verhindern, dass eine Evaluierung durch ungebührliche Einflussnahme unzulässig beeinflusst wird, ist eine gewisse Trennung der Rollen erforderlich. Dies bedeutet, dass die oben beschriebenen Rollen von verschiedenen Entitäten erfüllt werden, mit der Ausnahme, dass die Rollen des Entwicklers und Antragstellers von einer einzigen Entität erfüllt werden können.

Darüber hinaus erfordern einige Evaluierungen (z. B. die EAL1-Evaluierung) möglicherweise nicht, dass der Entwickler in das Projekt einbezogen wird. In diesem Fall ist es der Antragsteller, der dem Evaluator den TOE zur Verfügung stellt und den Evaluationsnachweis erstellt.

9.2.4 Allgemeines Evaluierungsmodell

Der Evaluierungsprozess besteht aus dem Evaluator, der die Eingabearbeitsaufgabe der Evaluierung, die Ausgabearbeitsaufgabe der Evaluierung und die Evaluierungsunteraufgaben durchführt. Bild 2 vermittelt einen Überblick über die Beziehung zwischen diesen Arbeitsaufgaben und Unteraufgaben.

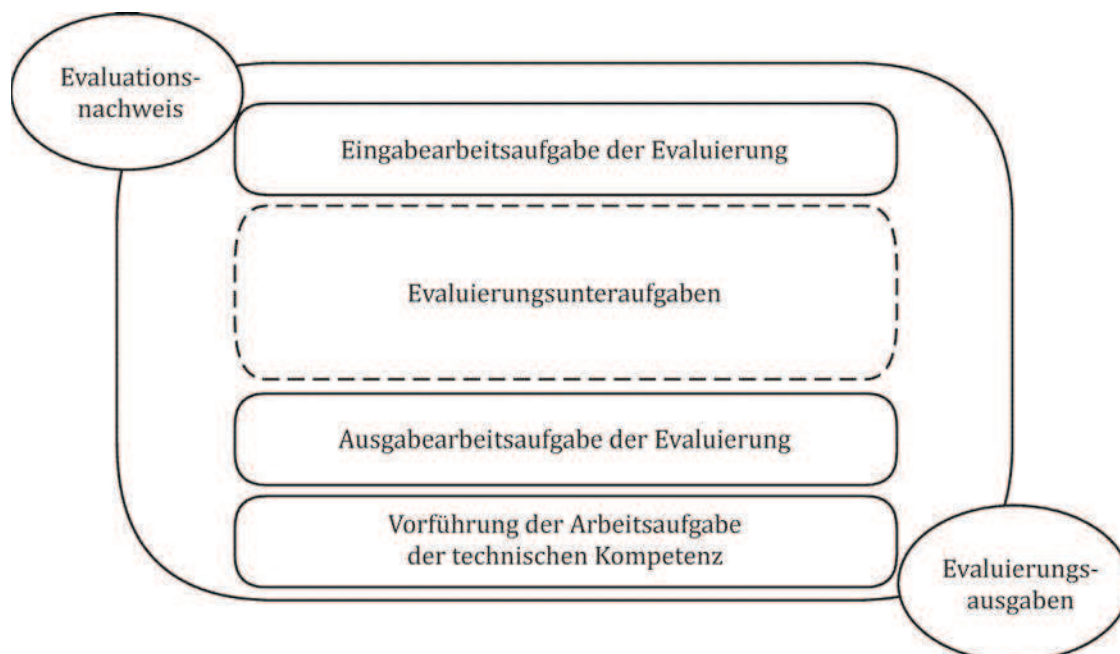


Bild 2 — Generisches Evaluierungsmodell

Dem Evaluierungsprozess kann eine Vorbereitungsphase vorausgehen, in der ein erster Kontakt zwischen dem Antragsteller und dem Evaluator hergestellt wird. Die Arbeit, die in dieser Phase geleistet wird, und die Einbeziehung der verschiedenen Rollen kann unterschiedlich sein. In der Regel führt der Evaluator während dieses Schritts eine Durchführbarkeitsanalyse durch, um die Wahrscheinlichkeit einer erfolgreichen Evaluierung zu beurteilen.

9.2.5 Evaluatoren-Entscheidungen

Der Evaluator ordnet die Entscheidungen den Anforderungen aus ISO/IEC 15408 und nicht denen aus diesem Dokument zu. Die kleinste Einheit der Struktur aus ISO/IEC 15408, der eine Entscheidung zugeordnet wird, ist das Evaluatorenaktionselement (explizit oder implizit). Eine Entscheidung wird einem zutreffenden Evaluatorenaktionselement aus ISO/IEC 15408 als Ergebnis der Durchführung der entsprechenden Aktion der Evaluierungsmethodik und der Workunits zugeordnet, aus denen sie besteht. Wenn es die Sicherheitsvorgaben erfordern, kann der Evaluator die aus den Workunits dieses Dokuments abgeleiteten Evaluierungsaufgaben durchführen (z. B. unter Verwendung des Rahmenwerks in ISO/IEC 15408-4:2022). Wenn solche abgeleiteten Evaluierungsverfahren und Evaluierungsaufgaben von einer ST gefordert werden, müssen diese vom Evaluator verwendet werden, um dem/den entsprechenden Evaluatorenaktions-element(en) Entscheidungen zuzuordnen. Schließlich wird ein Evaluierungsergebnis zugeordnet, wie in ISO/IEC 15408-1:2022, Abschnitt 13, Evaluierung und Evaluierungsergebnisse, beschrieben.

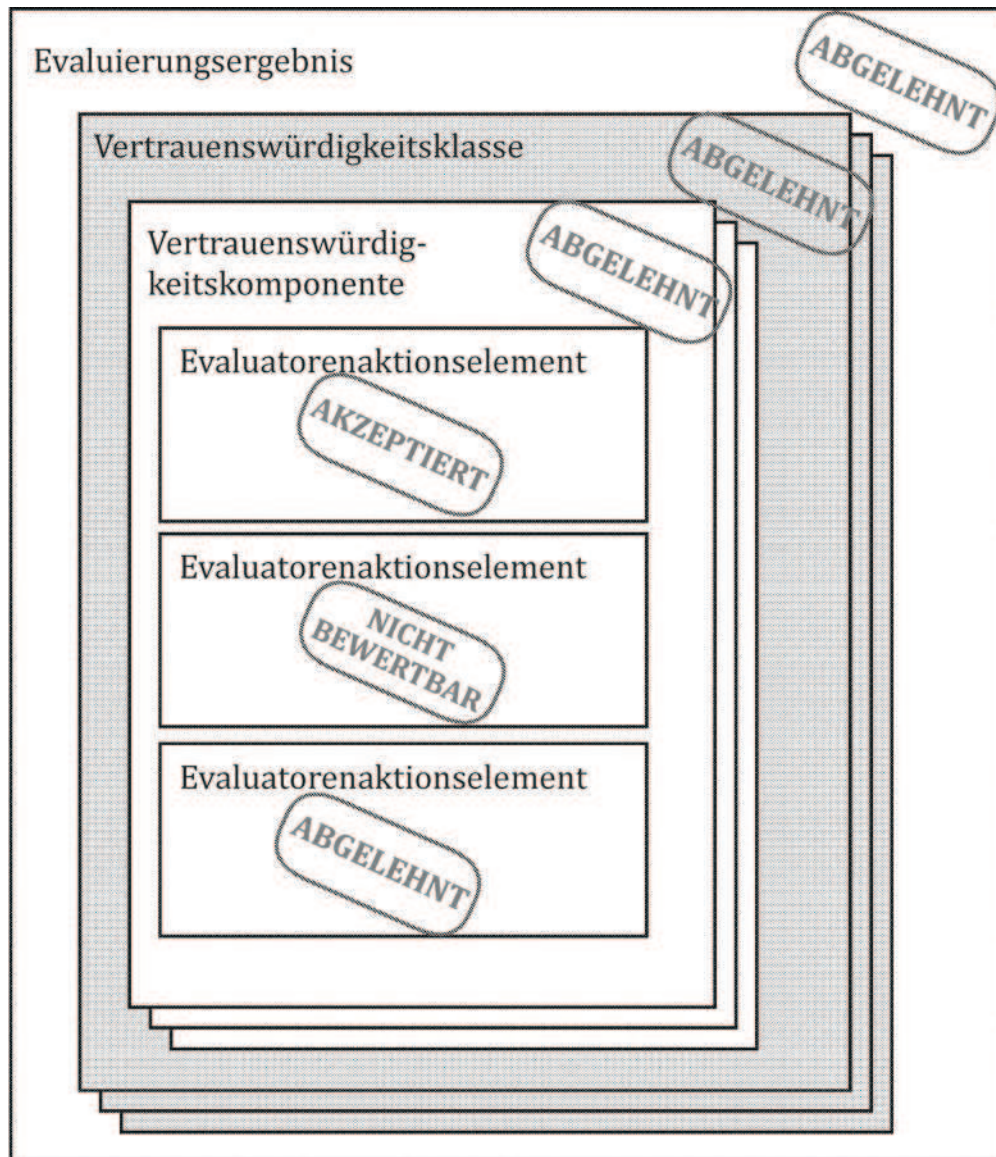


Bild 3 — Beispiel der Entscheidungszuordnungsregel

Dieses Dokument erkennt drei sich gegenseitig ausschließende Entscheidungszustände an:

- a) Die Bedingungen für eine „akzeptiert“-Entscheidung sind definiert als die Vervollständigung des Evaluatorenaktionselements aus ISO/IEC 15408 durch den Evaluator und die Feststellung, dass die Anforderungen an das/die zu evaluierende PP, PP-Konfiguration, ST oder den TOE erfüllt sind. Die Bedingungen für die Übergabe des Elements sind definiert als:
 - 1) die einzelnen Workunits der entsprechenden Aktion der Evaluierungsmethodologie, und
 - 2) alle für die Durchführung dieser Workunits erforderlichen Evaluationsnachweise sind einheitlich, d. h. sie können vom Evaluator vollständig verstanden werden, und

- 3) alle für die Durchführung dieser Workunits erforderlichen Evaluationsnachweise weisen keine offensichtlichen internen Inkonsistenzen oder Widersprüche zu anderen Evaluationsnachweisen auf. Es ist zu beachten, dass hier offensichtlich bedeutet, dass der Evaluator diese Inkonsistenz bei der Durchführung der Workunits entdeckt: Der Evaluator sollte nicht jedes Mal, wenn eine Workunit durchgeführt wird, eine vollständige Konsistenzanalyse über die gesamten Evaluationsnachweise hinweg durchführen;
- b) die Bedingungen für eine „*abgelehnt*“-Entscheidung sind definiert als eine Vervollständigung des Evaluatorenaktionselements aus ISO/IEC 15408 durch den Evaluator und die Feststellung, dass die Anforderungen an das/die zu evaluierende PP, PP-Konfiguration, ST oder den TOE nicht erfüllt sind oder eine offensichtliche Inkonsistenz in den Evaluationsnachweisen festgestellt wurde;
- c) alle Entscheidungen sind zunächst *nicht bewertbar* und bleiben so lange bestehen, bis entweder eine „*akzeptiert*“- oder „*abgelehnt*“-Entscheidung zugewiesen wird.

Die Gesamtentscheidung ist genau dann „*akzeptiert*“, wenn sämtliche einzelnen Entscheidungen auch „*akzeptiert*“ sind. Wenn in dem in Bild 3 dargestellten Beispiel die Entscheidung für ein Evaluatorenaktionselement „*abgelehnt*“ ist, sind auch die Entscheidungen für die entsprechende Vertrauenswürdigkeitskomponente, die Vertrauenswürdigkeitsklasse und die Gesamtentscheidung „*abgelehnt*“.

9.3 Eingebearbeitungsaufgabe der Evaluierung

9.3.1 Zielsetzungen

Die Zielsetzung dieser Arbeitsaufgabe ist es, sicherzustellen, dass der Evaluator über die richtige Version der für die Evaluierung erforderlichen Evaluationsnachweise verfügt und dass diese angemessen geschützt sind. Andernfalls kann weder die technische Genauigkeit der Evaluierung noch die Wiederholbarkeit und Reproduzierbarkeit der Ergebnisse der Evaluierung sichergestellt werden.

9.3.2 Anwendungshinweise

Die Verantwortung für die Bereitstellung aller erforderlichen Evaluationsnachweise liegt beim Antragsteller. Jedoch werden wahrscheinlich die meisten Evaluationsnachweise vom Entwickler im Auftrag des Antragstellers erstellt und geliefert.

Da die Vertrauenswürdigkeitsanforderungen für den gesamten TOE gelten, sind dem Evaluator alle Evaluationsnachweise, die sich auf alle Teile des TOE beziehen, zur Verfügung zu stellen. Der Umfang und der erforderliche Inhalt solcher Evaluationsnachweise ist unabhängig von dem Grad der Kontrolle, die der Entwickler über jeden der Teile des TOE hat. Wenn zum Beispiel ein Design erforderlich ist, dann gelten die Anforderungen des „TOE design“ (ADV_TDS) für alle Teilsysteme, die Teil der TSF sind. Darüber hinaus gelten Vertrauenswürdigkeitsanforderungen, die vorhandene Verfahren erfordern (z. B. „CM capabilities“ (ALC_CMC) und „Delivery“ (ALC_DEL), auch für den gesamten TOE (einschließlich aller Teile, die von einem anderen Entwickler hergestellt wurden).

Es wird empfohlen, dass der Evaluator in Zusammenarbeit mit dem Antragsteller einen Index zu den erforderlichen Evaluationsnachweisen erstellt. Dieser Index kann eine Menge Verweisungen auf die Dokumentation sein. Dieser Index sollte genügend Informationen enthalten (z. B. eine kurze Zusammenfassung jedes Dokuments oder zumindest einen expliziten Titel, die Angabe der relevanten Unterabschnitte), damit der Evaluator die erforderlichen Nachweise leicht findet.

Erforderlich sind die in den Evaluationsnachweisen enthaltenen Informationen, nicht eine bestimmte Dokumentenstruktur. Der Evaluationsnachweis für eine Unteraufgabe kann durch getrennte Dokumente erbracht werden, oder ein einziges Dokument kann mehrere der Eingabeanforderungen einer Unteraufgabe erfüllen.

Der Evaluator benötigt stabile und offiziell herausgegebene Versionen der Evaluationsnachweise. Der Entwurf eines Evaluationsnachweises kann jedoch während einer Evaluierung vorgelegt werden, z. B. um einem Evaluator eine frühzeitige, informelle Beurteilung zu ermöglichen, dieser wird aber nicht als Grundlage für Entscheidungen verwendet. Es kann für den Evaluator hilfreich sein, Entwürfe von besonders geeigneten Evaluationsnachweisen zu sehen, wie z. B.:

- a) eine Prüfdokumentation, um dem Evaluator eine frühzeitige Beurteilung von Prüfungen und Prüfverfahren zu ermöglichen;
- b) Designunterlagen, um dem Evaluator den Hintergrund für das Verständnis des TOE-Designs zu vermitteln;
- c) Quellcode oder Hardware-Zeichnungen, damit der Evaluator die Anwendung der Normen des Entwicklers beurteilen kann.

Der Entwurf eines Evaluationsnachweises wird mit größerer Wahrscheinlichkeit dann angetroffen, wenn die Evaluierung eines TOE gleichzeitig mit seiner Entwicklung durchgeführt wird. Er kann jedoch auch während der Evaluierung eines bereits entwickelten TOE auftreten, wenn der Entwickler zusätzliche Arbeiten durchführen musste, um ein vom Evaluator erkanntes Problem zu beheben (z. B. um einen Fehler im Design oder in der Implementierung zu beheben) oder um einen Evaluationsnachweis für die Sicherheit zu erbringen, der nicht in der vorhandenen Dokumentation enthalten ist (z. B. im Fall eines TOE, der ursprünglich nicht entwickelt wurde, um die Anforderungen von ISO/IEC 15408 zu erfüllen).

9.3.3 Management der Teilarbeitsaufgabe der Evaluationsnachweise

9.3.3.1 Konfigurationsüberwachung

Der Evaluator **muss** die Konfigurationsüberwachung der Evaluationsnachweise **durchführen**.

Die ISO/IEC 15408 impliziert, dass der Evaluator in der Lage ist, jeden Evaluationsnachweis nach dessen Erhalt zu identifizieren und zu lokalisieren und festzustellen, ob sich eine bestimmte Version eines Dokuments im Besitz des Evaluators befindet.

Der Evaluator **muss** die Evaluationsnachweise vor Änderungen oder Verlust **schützen**, solange sie sich im Besitz des Evaluators befinden.

9.3.3.2 Beseitigung

Es kann sein, dass Schemata die Beseitigung von Evaluationsnachweisen am Ende einer Evaluierung kontrollieren wollen. Die Beseitigung der Evaluationsnachweise sollte durch einen oder mehrere folgender Punkte erreicht werden:

- a) Rückgabe der Evaluationsnachweise;
- b) Archivierung der Evaluationsnachweise;
- c) Vernichtung der Evaluationsnachweise.

9.3.3.3 Vertraulichkeit

Ein Evaluator kann Zugriff auf kommerziell sensible Informationen des Antragstellers und des Entwicklers haben (z. B. Informationen über das TOE-Design, spezielle Instrumente), und er kann während des Verlaufs einer Evaluierung Zugriff auf national sensible Informationen haben. Es kann sein, dass Schemata Anforderungen an den Evaluator stellen wollen, um die Vertraulichkeit der Evaluationsnachweise zu wahren. Antragsteller und Evaluator können sich gegenseitig auf zusätzliche Anforderungen einigen, solange diese gegenüber dem Schema konsistent sind.

Die Anforderungen an die Vertraulichkeit betreffen viele Aspekte bei der Durchführung der Evaluierung, einschließlich der Entgegennahme, Handhabung, Lagerung und Beseitigung von Evaluationsnachweisen.

9.4 Evaluierungsunteraufgaben

Die Evaluierungsunteraufgaben unterscheiden sich je nachdem, ob es sich um ein PP, eine PP-Konfiguration oder eine TOE-Evaluierung handelt. Darüber hinaus hängen im Fall einer TOE-Evaluierung die Unteraufgaben von den gewählten Vertrauenswürdigkeitsanforderungen ab.

9.5 Ausgabearbeitsaufgabe der Evaluierung

9.5.1 Zielsetzungen

Die Zielsetzung dieses Unterabschnitts ist es, den Beobachtungsbericht (OR) und den Technischen Evaluierungsbericht (ETR) zu beschreiben. Die Schemata können zusätzliche Berichte des Evaluatoren, wie z. B. Berichte über einzelne Workunits, oder zusätzliche Informationen im OR und im ETR verlangen. Dieses Dokument schließt die zusätzliche Aufnahme von Informationen in diese Berichte nicht aus, da diese Internationale Norm nur den Mindestinformationsgehalt festlegt.

Eine konsistente Berichterstattung über die Evaluierungsergebnisse erleichtert das Erreichen des universellen Prinzips der Wiederholbarkeit und Reproduzierbarkeit der Ergebnisse. Die Konsistenz umfasst die Art und den Umfang der im ETR und OR gemeldeten Informationen. Die Konsistenz von ETR und OR zwischen den verschiedenen Evaluierungen liegt in der Verantwortung der Evaluierungsinstanz.

Der Evaluator führt die beiden folgenden Teilarbeitsaufgaben durch, um die Anforderungen dieses Dokuments an den Informationsgehalt von Berichten zu erfüllen:

- a) OR-Teilarbeitsaufgabe schreiben (falls im Zusammenhang mit der Evaluierung benötigt);
- b) ETR-Teilarbeitsaufgabe schreiben.

9.5.2 Management der Evaluierungsausgaben

Der Evaluator liefert den ETR an die Evaluierungsinstanz sowie alle OR, sobald sie verfügbar sind. Die Anforderungen an die Kontrolle des Umgangs mit dem ETR und den OR werden durch das Schema festgelegt, das auch die Lieferung an den Antragsteller oder Entwickler umfassen kann. Der ETR und die OR können sensible oder geschützte Informationen enthalten und müssen möglicherweise vor der Weitergabe an den Antragsteller zensiert werden.

9.5.3 Anwendungshinweise

In dieser Ausgabe dieses Dokuments wurden die Anforderungen an die Bereitstellung von Evaluationsnachweisen zur Unterstützung der Neubewertung und Wiederverwendung nicht explizit angegeben. Wenn der Antragsteller Informationen zur Neubewertung oder Wiederverwendung benötigt, sollte das Schema, nach dem die Evaluierung durchgeführt wird, konsultiert werden.

9.5.4 OR-Teilarbeitsaufgabe schreiben

Die OR bieten dem Evaluator einen Mechanismus, mit dem er eine Klarstellung (z. B. von der Evaluierungsinstanz über die Anwendung einer Anforderung) oder die Ermittlung eines Problems mit einem Aspekt der Evaluierung anfragt.

Im Falle einer ablehnenden Entscheidung **muss** der Evaluator einen OR **vorlegen**, der das Evaluierungsergebnis widerspiegelt. Andernfalls kann der Evaluator die OR als eine Möglichkeit nutzen, um den Klärungsbedarf auszudrücken.

Bei jedem OR **muss** der Evaluator Folgendes **angeben**:

- a) den Bezeichner des evaluierten PP oder TOE;
- b) die Evaluierungsarbeitsaufgabe/-Unteraufgabe, während der die Beobachtung gemacht wurde;
- c) die Beobachtung;
- d) die Beurteilung ihres Schweregrades (z. B. impliziert eine ablehnende Entscheidung, verzögert den Fortschritt der Evaluierung, erfordert eine Lösung vor Abschluss der Evaluierung);
- e) die Identifizierung der für die Lösung des Problems verantwortlichen Organisation;
- f) den empfohlenen Zeitplan für die Lösung;
- g) die Beurteilung der Auswirkung auf die Evaluierung des Versäumnisses, die Beobachtung zu lösen.

Die angesprochene Zielgruppe eines OR und Verfahren zur Handhabung des Berichts hängen von der Art des Berichtsinhalts und vom Schema ab. Die Schemata können verschiedene Arten von OR unterscheiden oder zusätzliche Typen definieren, mit den damit verbundenen Unterschieden bei den erforderlichen Informationen und der Verteilung (z. B. Evaluierungs-OR an Evaluierungsinstanzen und Antragsteller).

9.5.5 ETR-Teilarbeitsaufgabe schreiben

9.5.5.1 Zielsetzungen

Der Evaluator **muss** einen ETR **bereitstellen**, um die technische Begründung der Entscheidungen vorzulegen.

Dieses Dokument definiert die Mindestanforderung an den Inhalt des ETR; die Schemata können jedoch zusätzliche Inhalte und spezifische Anforderungen an die Darstellung und Struktur festlegen. Beispielsweise können die Schemata verlangen, dass bestimmte einleitende Ausführungen (z. B. Haftungsausschlüsse und Urheberrechtshinweise) im ETR gemeldet werden.

Es wird davon ausgegangen, dass der Leser des ETR mit den allgemeinen Konzepten der IT-Sicherheit, von ISO/IEC 15408, dieses Dokuments, den Evaluierungsansätzen und der IT vertraut ist.

Der ETR unterstützt die Evaluierungsinstanz bei der Bestätigung, dass die Evaluierung nach der geforderten Norm durchgeführt wurde, aber es wird erwartet, dass die dokumentierten Ergebnisse möglicherweise nicht alle erforderlichen Informationen enthalten, so dass zusätzliche, vom Schema speziell angefragte Informationen erforderlich sein können. Dieser Aspekt liegt außerhalb des Anwendungsbereichs dieses Dokuments.

9.5.5.2 ETR für eine PP-Evaluierung

9.5.5.2.1 Allgemeines

In diesem Unterabschnitt wird der Mindestinhalt des ETR für eine PP-Evaluierung beschrieben. Der Inhalt des ETR ist in Bild 4 dargestellt; dieses Bild kann als Anleitung beim Aufbau der Struktur des ETR-Dokuments verwendet werden.

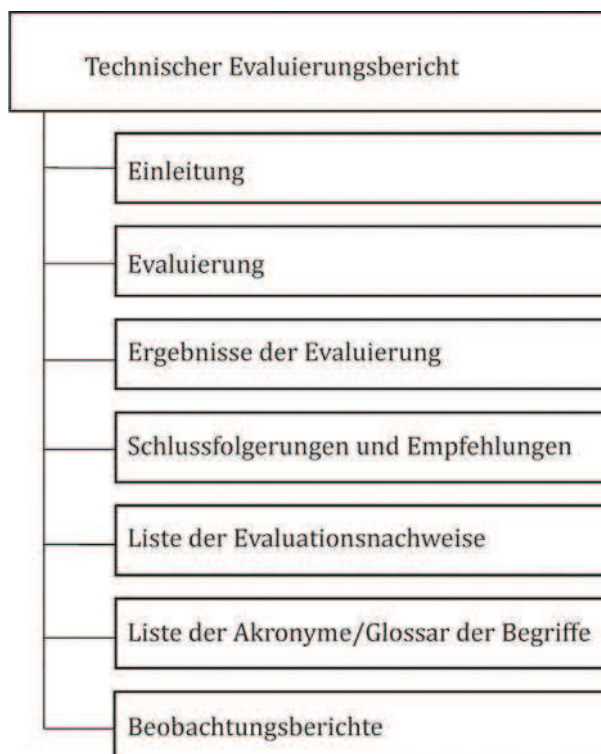


Bild 4 — ETR-Informationsgehalt für eine PP-Evaluierung

9.5.5.2.2 Allgemeines

Der Evaluator **muss** die Schemabezeichner der Evaluierung **angeben**.

Schemabezeichner der Evaluierung (z. B. Logos) sind die Informationen, die erforderlich sind, um das für die Überwachung der Evaluierung verantwortliche Schema eindeutig zu identifizieren.

Der Evaluator **muss** die ETR-Bezeichner der Konfigurationsüberwachung **angeben**.

Die ETR-Bezeichner der Konfigurationsüberwachung enthalten Informationen, die den ETR identifizieren (z. B. Name, Datum und Versionsnummer).

Der Evaluator **muss** die PP-Bezeichner der Konfigurationsüberwachung **angeben**.

PP-Bezeichner der Konfigurationsüberwachung (z. B. Name, Datum und Versionsnummer) sind erforderlich, um zu identifizieren, was evaluiert wird, damit die Evaluierungsinstanz überprüfen kann, ob die Entscheidungen vom Evaluator korrekt zugeordnet wurden.

Der Evaluator **muss** die Identität des Entwicklers **angeben**.

Die Identität des PP-Entwicklers wird benötigt, um die verantwortliche Partei für die Erstellung des PP zu identifizieren.

Der Evaluator **muss** die Identität des Antragstellers **angeben**.

Die Identität des Antragstellers wird benötigt, um die verantwortliche Partei zu identifizieren, die für die Bereitstellung von Evaluationsnachweisen für den Evaluator verantwortlich ist.

Der Evaluator **muss** die Identität des Evaluators **angeben**.

Die Identität des Evaluators wird benötigt, um die Partei zu identifizieren, die die Evaluierung durchführt und für die Evaluierungsentscheidungen verantwortlich ist.

9.5.5.2.3 Evaluierung

Der Evaluator **muss** die Evaluierungsverfahren, -techniken, -instrumente und angewandten Normen **angeben**.

Der Evaluator verweist auf die Evaluierungskriterien, die Methodik und die Interpretationen, die zur Evaluierung des PP verwendet wurden.

Der Evaluator **muss** alle Einschränkungen bei der Evaluierung, Einschränkungen bei der Handhabung der Evaluierungsergebnisse und Annahmen **angeben**, die während der Evaluierung getroffen wurden und sich auf die Evaluierungsergebnisse auswirken.

Der Evaluator kann Informationen in Bezug auf rechtliche oder gesetzliche Aspekte, Organisation, Vertraulichkeit einbeziehen.

9.5.5.2.4 Ergebnisse der Evaluierung

Der Evaluator **muss** eine Entscheidung und eine unterstützende Begründung für jede Vertrauenswürdigkeitskomponente **angeben**, die eine APE-Aufgabe ausmacht, als Ergebnis der Durchführung der entsprechenden Aktion der Evaluierungsmethodik und der Workunits, aus denen sie besteht.

Die Begründung legt die Entscheidung unter Verwendung von ISO/IEC 15408, dieses Dokuments, etwaiger Interpretationen und der untersuchten Evaluationsnachweise dar und zeigt, wie die Evaluationsnachweise jeden Aspekt der Kriterien erfüllen oder nicht. Sie enthält eine Beschreibung der ausgeführten Arbeiten, der angewandten Verfahren und jede Herleitung von Ergebnissen. Die Begründung kann bis auf die Ebene einer Workunit der Evaluierungsmethodik detailliert sein.

9.5.5.2.5 Schlussfolgerungen und Empfehlungen

Der Evaluator **muss** die Schlussfolgerungen der Evaluierung, insbesondere die Gesamtentscheidung **angeben**, wie in ISO/IEC 15408-1:2022, Abschnitt 12, Evaluierungsergebnisse, festgelegt, und durch die Anwendung der in 8.2.5 beschriebenen Entscheidungszuordnung bestimmt.

Der Evaluator gibt Empfehlungen, die für die Evaluierungsinstanz hilfreich sein können. Diese Empfehlungen können Defizite des PP, die bei der Evaluierung festgestellt wurden, oder die Erwähnung von besonders nützlichen Funktionen beinhalten.

9.5.5.2.6 Liste der Evaluationsnachweise

Der Evaluator **muss** für jeden einzelnen Evaluationsnachweis die folgenden Informationen **angeben**:

- a) die Ausgabestelle (z. B. der Entwickler, der Antragsteller);
- b) den Titel;
- c) die eindeutige Verweisung (z. B. Ausgabedatum und Versionsnummer).

9.5.5.2.7 Liste der Akronyme/Glossar der Begriffe

Der Evaluator **muss** sämtliche im ETR verwendeten Akronyme oder Abkürzungen **angeben**:

Von ISO/IEC 15408 (alle Teile) oder diesem Dokument bereits festgelegte Glossardefinitionen müssen im ETR nicht wiederholt werden.

9.5.5.2.8 Beobachtungsberichte

Der Evaluator **muss** eine vollständige Liste **angeben**, aus der die bei der Evaluierung erhobenen OR und ihr Status eindeutig hervorgehen.

Für jeden OR sollte die Liste dessen Bezeichner sowie seinen Titel oder eine kurze Zusammenfassung seines Inhalts enthalten.

9.5.5.3 ETR für die Evaluierung einer PP-Konfiguration

9.5.5.3.1 Allgemeines

In diesem Unterabschnitt wird der Mindestinhalt des ETR für die Evaluierung einer PP-Konfiguration beschrieben. Der Inhalt des ETR ist in Bild 5 dargestellt; dieses Bild kann als Anleitung beim Aufbau der Struktur des ETR-Dokuments verwendet werden.

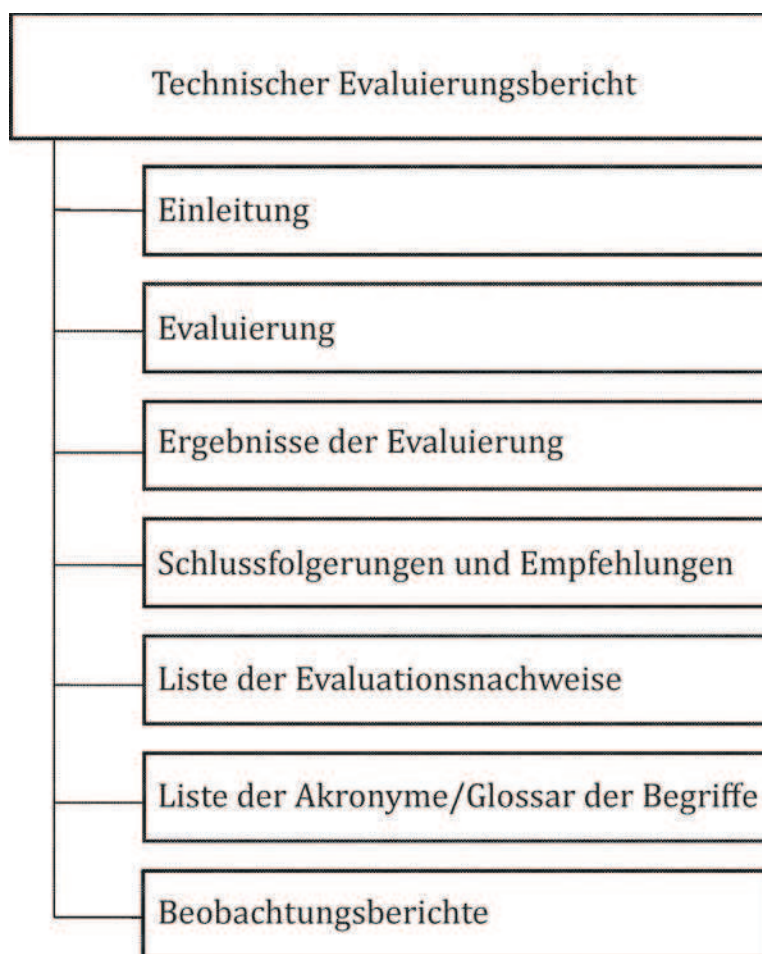


Bild 5 — ETR-Informationsgehalt für eine PP-Evaluierung

9.5.5.3.2 Allgemeines

Der Evaluator **muss** die Schemabezeichner der Evaluierung **angeben**.

Schemabezeichner der Evaluierung (z. B. Logos) sind die Informationen, die erforderlich sind, um das für die Überwachung der Evaluierung verantwortliche Schema eindeutig zu identifizieren.

Der Evaluator **muss** die ETR-Bezeichner der Konfigurationsüberwachung **angeben**.

Die ETR-Bezeichner der Konfigurationsüberwachung enthalten Informationen, die den ETR identifizieren (z. B. Name, Datum und Versionsnummer).

Der Evaluator **muss** die Bezeichner der Konfigurationsüberwachung für die PP-Konfiguration **angeben**.

PP-Bezeichner der Konfigurationsüberwachung (z. B. Name, Datum und Versionsnummer) sind erforderlich, um zu identifizieren, was evaluiert wird, damit die Evaluierungsinstanz überprüfen kann, ob die Entscheidungen vom Evaluator korrekt zugeordnet wurden.

Der Evaluator **muss** die Identität des Entwicklers **angeben**.

Die Identität des Entwicklers der PP-Konfiguration wird benötigt, um die verantwortliche Partei für die Erstellung der PP-Konfiguration zu identifizieren.

Der Evaluator **muss** die Identität des Antragstellers **angeben**.

Die Identität des Antragstellers wird benötigt, um die verantwortliche Partei zu identifizieren, die für die Bereitstellung von Evaluationsnachweisen für den Evaluator verantwortlich ist.

Der Evaluator **muss** die Identität des Evaluators **angeben**.

Die Identität des Evaluators wird benötigt, um die Partei zu identifizieren, die die Evaluierung durchführt und für die Evaluierungsentscheidungen verantwortlich ist.

9.5.5.3.3 Überblick über die PP-Konfiguration

Der Evaluator **muss** alle in der PP-Konfiguration verwendeten Komponenten der PP-Konfiguration **angeben**.

Zu den Komponenten der PP-Konfiguration gehören mindestens ein PP sowie alle anderen in der PP-Konfiguration verwendeten PP und PP-Module. Zu jedem PP-Modul wird eine seiner PP-Modulbasen in die PP-Konfiguration aufgenommen, so dass alle Elemente der jeweiligen PP-Modulbasis als Komponenten der PP-Konfiguration enthalten sind. Siehe ISO/IEC 15408-1:2022, Anhang C, für weitere Einzelheiten zur Identifizierung der PP-Modulbasis für jedes PP-Modul.

Der ETR **muss** die Verweisung auf die Komponenten der PP-Konfiguration **angeben**.

Eine Verweisung auf die Komponenten der PP-Konfiguration enthält Informationen, die die spezifische Komponente eindeutig identifizieren (z. B. Titel, Datum und Versionsnummer).

9.5.5.3.4 Evaluierung

Der Evaluator **muss** die Evaluierungsverfahren, -techniken, -instrumente und angewandten Normen **angeben**.

Der Evaluator verweist auf die Evaluierungskriterien, die Methodik und die Interpretationen, die zur Evaluierung der PP-Konfiguration verwendet wurden.

Der Evaluator **muss** alle Einschränkungen bei der Evaluierung, Einschränkungen bei der Handhabung der Evaluierungsergebnisse und Annahmen **angeben**, die während der Evaluierung getroffen wurden und sich auf die Evaluierungsergebnisse auswirken.

Der Evaluator kann Informationen in Bezug auf rechtliche oder gesetzliche Aspekte, Organisation, Vertraulichkeit einbeziehen.

9.5.5.3.5 Ergebnisse der Evaluierung

Der Evaluator **muss** eine Entscheidung und eine unterstützende Begründung für jede Vertrauenswürdigkeitskomponente **angeben**, die eine ACE-Aufgabe ausmacht, als Ergebnis der Durchführung der entsprechenden Aktion der Evaluierungsmethodik und der Workunits, aus denen sie besteht.

Die Begründung legt die Entscheidung unter Verwendung von ISO/IEC 15408, dieses Dokuments, etwaiger Interpretationen und der untersuchten Evaluationsnachweise dar und zeigt, wie die Evaluationsnachweise jeden Aspekt der Kriterien erfüllen oder nicht. Sie enthält eine Beschreibung der ausgeführten Arbeiten, der angewandten Verfahren und jede Herleitung von Ergebnissen. Die Begründung kann bis auf die Ebene einer Workunit der Evaluierungsmethodik detailliert sein.

9.5.5.3.6 Schlussfolgerungen und Empfehlungen

Der Evaluator **muss** die Schlussfolgerungen der Evaluierung, insbesondere die Gesamtentscheidung **angeben**, wie in ISO/IEC 15408-1:2022 Abschnitt 12, Evaluierungsergebnisse, festgelegt, und durch die Anwendung der in 8.2.5 beschriebenen Entscheidungszuordnung bestimmt.

Der Evaluator gibt Empfehlungen, die für die Evaluierungsinstanz hilfreich sein können. Diese Empfehlungen können Defizite der PP-Konfiguration, die bei der Evaluierung festgestellt wurden, oder die Erwähnung von besonders nützlichen Funktionen beinhalten.

9.5.5.3.7 Liste der Evaluationsnachweise

Der Evaluator **muss** für jeden einzelnen Evaluationsnachweis die folgenden Informationen **angeben**:

- a) die Ausgabestelle (z. B. der Entwickler, der Antragsteller);
- b) den Titel;
- c) die eindeutige Verweisung (z. B. Ausgabedatum und Versionsnummer).

9.5.5.3.8 Liste der Akronyme/Glossar der Begriffe

Der Evaluator **muss** sämtliche im ETR verwendeten Akronyme oder Abkürzungen **angeben**.

Von ISO/IEC 15408 oder diesem Dokument bereits festgelegte Glossardefinitionen müssen im ETR nicht wiederholt werden.

9.5.5.3.9 Beobachtungsberichte

Der Evaluator **muss** eine vollständige Liste **angeben**, aus der die bei der Evaluierung erhobenen OR und ihr Status eindeutig hervorgehen.

Für jeden OR sollte die Liste dessen Bezeichner sowie seinen Titel oder eine kurze Zusammenfassung seines Inhalts enthalten.

9.5.5.4 ETR für eine TOE-Evaluierung

9.5.5.4.1 Allgemeines

In diesem Unterabschnitt wird der Mindestinhalt des ETR für eine TOE-Evaluierung beschrieben. Der Inhalt des ETR ist in Bild 6 dargestellt; dieses Bild kann als Anleitung beim Aufbau der Struktur des ETR-Dokuments verwendet werden.

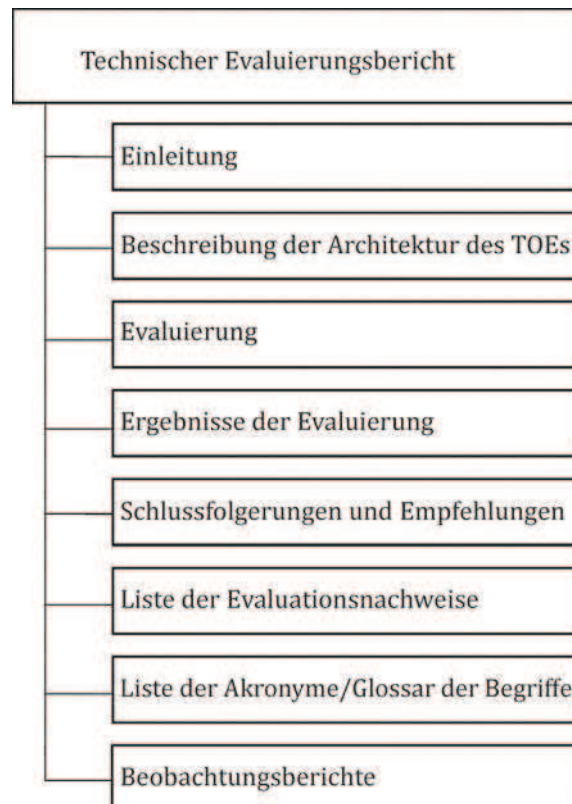


Bild 6 — ETR-Informationsgehalt für eine TOE-Evaluierung

9.5.5.4.2 Allgemeines

Der Evaluator **muss** die Schemabezeichner der Evaluierung **angeben**.

Schemabezeichner der Evaluierung (z. B. Logos) sind die Informationen, die erforderlich sind, um das für die Überwachung der Evaluierung verantwortliche Schema eindeutig zu identifizieren.

Der Evaluator **muss** die ETR-Bezeichner der Konfigurationsüberwachung **angeben**.

Die ETR-Bezeichner der Konfigurationsüberwachung enthalten Informationen, die den ETR identifizieren (z. B. Name, Datum und Versionsnummer).

Der Evaluator **muss** die ST- und TOE-Bezeichner der Konfigurationsüberwachung **angeben**.

ST- und TOE-Bezeichner der Konfigurationsüberwachung identifizieren, was evaluiert wird, damit die Evaluierungsinstanz überprüfen kann, ob die Entscheidungen vom Evaluator korrekt zugeordnet wurden.

Wenn die ST beansprucht, dass der TOE mit den Anforderungen eines oder mehrerer PP bzw. einer PP-Konfiguration übereinstimmt, muss der ETR die Verweisung der entsprechenden PP/PP-Konfiguration melden.

Die Verweisung der PP/PP-Konfiguration enthält Informationen, die die PP/PP-Konfiguration eindeutig identifizieren (z. B. Titel, Datum und Versionsnummer).

Der Evaluator **muss** die Identität des Entwicklers **angeben**.

Die Identität des TOE-Entwicklers wird benötigt, um die verantwortliche Partei für die Erstellung des TOE zu identifizieren.

Der Evaluator **muss** die Identität des Antragstellers **angeben**.

Die Identität des Antragstellers wird benötigt, um die verantwortliche Partei zu identifizieren, die für die Bereitstellung von Evaluationsnachweisen für den Evaluator verantwortlich ist.

Der Evaluator **muss** die Identität des Evaluators **angeben**.

Die Identität des Evaluators wird benötigt, um die Partei zu identifizieren, die die Evaluierung durchführt und für die Evaluierungsentscheidungen verantwortlich ist.

9.5.5.4.3 Beschreibung der Architektur des TOE

Der Evaluator **muss**, soweit zutreffend, eine allgemeine Beschreibung des TOE und seiner Hauptkomponenten auf der Grundlage der in der ISO/IEC 15408 Vertrauenswürdigkeitsfamilie beschriebenen Evaluationsnachweise mit dem Titel „TOE design“ (ADV_TDS) **angeben**.

Ziel dieses Unterabschnitts ist es, den Grad der architektonischen Trennung der Hauptkomponenten zu charakterisieren. Wenn es keine Anforderung „TOE design“ (ADV_TDS) in der ST gibt, ist dies nicht anwendbar und gilt als erfüllt.

9.5.5.4.4 Evaluierung

Der Evaluator **muss** die Evaluierungsverfahren, -techniken, -instrumente und angewandten Normen **angeben**.

Der Evaluator darf auf die Evaluierungskriterien, die Methodik und die Interpretationen verweisen, die zur Evaluierung des TOE oder der zur Durchführung der Prüfungen verwendeten Geräte verwendet werden. Dies muss die Identifizierung aller abgeleiteten Evaluierungsverfahren und Evaluierungsaufgaben einschließen, sowie eine Bestätigung, dass diese den Anforderungen der Sicherheitsvorgaben entsprechen (vgl. ASE_CCL).

Der Evaluator **muss** alle Einschränkungen bei der Evaluierung, Einschränkungen bei der Verteilung der Evaluierungsergebnisse und Annahmen **angeben**, die während der Evaluierung getroffen wurden und sich auf die Evaluierungsergebnisse auswirken.

Der Evaluator kann Informationen in Bezug auf rechtliche oder gesetzliche Aspekte, Organisation, Vertraulichkeit einbeziehen.

9.5.5.4.5 Ergebnisse der Evaluierung

Für jede Aufgabe, bei der der TOE evaluiert wird, **muss** der Evaluator Folgendes **angeben**:

- a) die Bezeichnung der in Betracht gezogenen Aufgabe;
- b) eine Entscheidung und eine unterstützende Begründung für jede Vertrauenswürdigkeitskomponente, die diese Aufgabe ausmacht, als Ergebnis der Durchführung der entsprechenden Aktion der Evaluierungsmethodik und der Workunits, aus denen sie besteht.

Die Begründung legt die Entscheidung unter Verwendung von ISO/IEC 15408, dieses Dokuments, aller abgeleiteten Evaluierungsverfahren und der von der ST geforderten Evaluierungsaufgaben, etwaiger Interpretationen und der untersuchten Evaluationsnachweise dar und zeigt, wie die Evaluationsnachweise jeden Aspekt der Kriterien erfüllen oder nicht. Sie enthält eine Beschreibung der ausgeführten Arbeiten, der angewandten Verfahren und jede Herleitung von Ergebnissen. Die Begründung kann bis auf die Ebene einer Workunit der Evaluierungsmethodik detailliert sein.

Der Evaluator **muss** sämtliche Informationen **angeben**, die von einer Workunit speziell benötigt werden.

Für die AVA- und ATE-Aufgaben wurden Workunits festgelegt, die die im ETR anzugebenden Informationen bestimmen.

9.5.5.4.6 Schlussfolgerungen und Empfehlungen

Der Evaluator **muss** die Schlussfolgerungen der Evaluierung **angeben**, die sich darauf beziehen, ob der TOE seine zugehörige ST erfüllt hat, insbesondere die Gesamtentscheidung nach ISO/IEC 15408-1:2022, Evaluierung und Evaluierungsergebnisse, die durch die Anwendung der in 8.2.5 beschriebenen Entscheidungszuordnung bestimmt wird.

Der Evaluator gibt Empfehlungen, die für die Evaluierungsinstanz hilfreich sein können. Diese Empfehlungen können Defizite des IT-Produkts, die bei der Evaluierung festgestellt wurden, oder die Erwähnung von besonders nützlichen Funktionen beinhalten.

9.5.5.4.7 Liste der Evaluationsnachweise

Der Evaluator **muss** für jeden einzelnen Evaluationsnachweis die folgenden Informationen **angeben**:

- a) die Ausgabestelle (z. B. der Entwickler, der Antragsteller);
- b) den Titel;
- c) die eindeutige Verweisung (z. B. Ausgabedatum und Versionsnummer).

9.5.5.4.8 Liste der Akronyme/Glossar der Begriffe

Der Evaluator **muss** sämtliche im ETR verwendeten Akronyme oder Abkürzungen **angeben**.

Von ISO/IEC 15408 oder diesem Dokument bereits festgelegte Glossardefinitionen müssen im ETR nicht wiederholt werden.

9.5.5.4.9 Beobachtungsberichte

Der Evaluator **muss** eine vollständige Liste **angeben**, aus der die bei der Evaluierung erhobenen OR und ihr Status eindeutig hervorgehen.

Für jeden OR sollte die Liste dessen Bezeichner sowie seinen Titel oder eine kurze Zusammenfassung seines Inhalts enthalten.

10 Klasse APE: Evaluierung des Schutzprofils

10.1 Allgemeines

In diesem Abschnitt wird die Evaluierung eines PP beschrieben. Die Anforderungen und die Methodik der PP-Evaluierung sind für jede PP-Evaluierung identisch, unabhängig von der EAL (oder anderen Anforderungen an die Vertrauenswürdigkeit), die im PP beansprucht wird. Die Evaluierungsmethodik in diesem Abschnitt basiert auf den Anforderungen an das PP, wie in ISO/IEC 15408-3:2022, Klasse APE, festgelegt.

Dieser Abschnitt sollte in Verbindung mit ISO/IEC 15408-1:2022, Anhang B und Anhang D, verwendet werden, da diese Anhänge die hier dargestellten Konzepte verdeutlichen und eine Vielzahl an Beispielen zeigen.

10.2 Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs

Bei der Evaluierung eines PP, das auf einem oder mehreren zertifizierten PPs basiert, kann es möglich sein, die Tatsache, dass diese PPs zertifiziert wurden, wieder zu verwenden. Das Potential für die Wiederverwendung des Ergebnisses eines zertifizierten PPs ist größer, wenn das zu evaluierende PP keine zusätzlichen Bedrohungen, OSPs, Sicherheitszielsetzungen und/oder Sicherheitsanforderungen zu denen des PP, dessen Konformität beansprucht wird, enthält. Wenn das zu evaluierende PP wesentlich mehr als das zertifizierte PP enthält, ist eine Wiederverwendung möglicherweise überhaupt nicht sinnvoll.

Dem Evaluator ist es gestattet, die Ergebnisse der PP-Evaluierung wiederzuverwenden, indem er bestimmte Analysen nur teilweise oder gar nicht durchführt, wenn diese Analysen oder Teile davon bereits im Rahmen der PP-Evaluierung durchgeführt wurden. Dabei sollte der Evaluator davon ausgehen, dass die Analysen im PP korrekt durchgeführt wurden.

Ein Beispiel wäre, wenn das PP, dessen Konformität beansprucht wird, eine Menge Sicherheitsanforderungen enthält und diese bei der Evaluierung als in sich konsistent bestimmt wurden. Wenn das zu evaluierende PP genau die gleichen Anforderungen verwendet, muss die Konsistenzanalyse bei der PP-Evaluierung nicht wiederholt werden. Wenn das zu evaluierende PP eine oder mehrere Anforderungen hinzufügt oder Operationen auf diese Anforderungen durchführt, muss die Analyse wiederholt werden. Es kann jedoch möglich sein, bei dieser Konsistenzanalyse Arbeit zu sparen, indem die Tatsache genutzt wird, dass die ursprünglichen Anforderungen in sich konsistent sind. Wenn die ursprünglichen Anforderungen in sich konsistent sind, muss der Evaluator nur feststellen, dass:

- a) die Menge aller neuen und/oder geänderten Anforderungen in sich konsistent ist; und
- b) die Menge aller neuen und/oder geänderten Anforderungen gegenüber den ursprünglichen Anforderungen konsistent ist.

Der Evaluator vermerkt im ETR jeweils, wo Analysen aus diesem Grund nicht oder nur teilweise durchgeführt werden.

10.3 PP-Einleitung (APE_INT)

10.3.1 Evaluierung der Unteraufgabe (APE_INT.1)

10.3.1.1 Zielsetzungen

Die Zielsetzung dieser Unteraufgabe besteht darin, festzustellen, ob das PP korrekt identifiziert wird und ob die PP-Verweisung und der TOE-Überblick miteinander konsistent sind.

10.3.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist:

- a) das PP.

10.3.1.3 Aktion APE_INT.1.1E

10.3.1.3.1 Allgemeines

ISO/IEC 15408-3:2022 APE_INT.1.1C: *Die PP-Einleitung muss eine PP-Verweisung und einen TOE-Überblick enthalten.*

10.3.1.3.2 Workunit APE_INT.1-1

Der Evaluator **muss prüfen**, dass die PP-Einleitung eine PP-Verweisung und einen TOE-Überblick enthält.

ISO/IEC 15408-3:2022 APE_INT.1.2C: *Die PP-Verweisung muss das PP eindeutig identifizieren.*

10.3.1.3.3 Workunit APE_INT.1-2

Der Evaluator **muss** die PP-Verweisung **untersuchen**, um festzustellen, dass sie das PP eindeutig identifiziert.

Der Evaluator stellt fest, dass die PP-Verweisung das PP selbst identifiziert, so dass es leicht von anderen PPs unterschieden werden kann, und dass sie auch jede Version des PP eindeutig identifiziert, z. B. unter Einbeziehung einer Versionsnummer und/oder eines Veröffentlichungsdatums.

Das PP sollte über ein Verweisungssystem verfügen, das in der Lage ist, eindeutige Verweisungen zu unterstützen (z. B. Verwendung von Zahlen, Buchstaben oder Daten).

ISO/IEC 15408-3:2022 APE_INT.1.3C: *Der TOE-Überblick muss die Verwendung und wesentliche Sicherheitsmerkmale des TOE zusammenfassen.*

10.3.1.3.4 Workunit APE_INT.1-3

Der Evaluator **muss** den TOE-Überblick **untersuchen**, um festzustellen, dass er die Verwendung und die wichtigsten Sicherheitsmerkmale des TOE beschreibt.

Der TOE-Überblick sollte kurz (d.h. in einigen Absätzen) die Verwendung und die wichtigsten Sicherheitsmerkmale beschreiben, die vom TOE erwartet werden. Der TOE-Überblick sollte Verbraucher und potentielle TOE-Entwickler in die Lage versetzen, schnell festzustellen, ob das PP für sie von Interesse ist.

Der Evaluator stellt fest, dass der Überblick für Entwickler und Verbraucher des TOE klar genug ist und ausreicht, um ihnen ein allgemeines Verständnis der beabsichtigten Verwendung und der wichtigsten Sicherheitsmerkmale des TOE zu vermitteln.

ISO/IEC 15408-3:2022 APE_INT.1.4C: *Der TOE-Überblick muss den TOE-Typ identifizieren.*

10.3.1.3.5 Workunit APE_INT.1-4

Der Evaluator **muss prüfen**, dass der TOE-Überblick den TOE-Typ identifiziert.

ISO/IEC 15408-3:2022 APE_INT.1.5C: *Der TOE-Überblick muss jede nicht im TOE enthaltene, aber für den TOE verfügbare Hardware/Software/Firmware identifizieren.*

10.3.1.3.6 Workunit APE_INT.1-5

Der Evaluator **muss** den TOE-Überblick **untersuchen**, um festzustellen, dass er jede nicht im TOE enthaltene, aber für den TOE verfügbare Hardware/Software/Firmware identifiziert.

Während einige TOEs eigenständig laufen können, benötigen andere TOEs (insbesondere Software-TOEs) zusätzliche Hardware, Software oder Firmware für den Betrieb. In diesem Unterabschnitt des PP listet der Autor des PP die gesamte Hardware, Software und/oder Firmware auf, die für den TOE zur Verfügung stehen wird, um auf ihm zu laufen.

Diese Identifizierung sollte so detailliert sein, dass potentielle Verbraucher und TOE-Entwickler feststellen können, ob ihr TOE mit der aufgeführten Hardware, Software und Firmware betrieben werden kann.

10.4 Konformitätsansprüche (APE_CCL)

10.4.1 Evaluierung der Unteraufgabe (APE_CCL.1)

10.4.1.1 Zielsetzungen

Die Zielsetzung dieser Unteraufgabe ist es, die Gültigkeit verschiedener Konformitätsansprüche zu bestimmen. Diese beschreiben die Konformität des PP mit ISO/IEC 15408, anderen PPs und Paketen.

10.4.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist/sind:

- a) das PP;
- b) das/die Paket(e), mit dem/denen das PP Konformität beansprucht.

10.4.1.3 Aktion APE_CCL.1.1E

10.4.1.3.1 Allgemeines

ISO/IEC 15408-3:2022 APE_CCL.1.1C: *Der Konformitätsanspruch muss die Ausgabe von ISO/IEC 15408 identifizieren, mit der das PP Konformität beansprucht.*

10.4.1.3.2 Workunit APE_CCL.1-1

Der Evaluator **muss prüfen**, ob der Konformitätsanspruch die Ausgabe von ISO/IEC 15408 identifiziert, mit der das PP Konformität beansprucht.

Der Evaluator stellt fest, dass der Konformitätsanspruch nach ISO/IEC 15408 die Ausgabe von ISO/IEC 15408 identifiziert, die zur Entwicklung dieses PP verwendet wurde. Diese sollte die Ausgabennummer von ISO/IEC 15408 und, sofern nicht die internationale englische Ausgabe von ISO/IEC 15408 verwendet wurde, die Sprache der verwendeten Ausgabe von ISO/IEC 15408 enthalten.

ISO/IEC 15408-3:2022 APE_CCL.1.2C: *Der Konformitätsanspruch muss die Konformität des PP mit ISO/IEC 15408-2 entweder als ISO/IEC 15408-2-konform oder ISO/IEC 15408-2-erweitert beschreiben.*

10.4.1.3.3 Workunit APE_CCL.1-2

Der Evaluator **muss prüfen**, ob der Konformitätsanspruch nach ISO/IEC 15408 entweder den Anspruch ISO/IEC 15408-2-konform oder ISO/IEC 15408-2-erweitert für das PP angibt.

ISO/IEC 15408-3:2022 APE_CCL.1.3C: *Der Konformitätsanspruch muss die Konformität des PP entweder als „ISO/IEC 15408-3-konform“ oder als „ISO/IEC 15408-3:2022-erweitert“ beschreiben.*

10.4.1.3.4 Workunit APE_CCL.1-3

Der Evaluator **muss prüfen**, ob der Konformitätsanspruch nach ISO/IEC 15408 entweder den Anspruch ISO/IEC 15408-3:2022-konform oder ISO/IEC 15408-3:2022-erweitert für das PP angibt.

ISO/IEC 15408-3:2022 APE_CCL.1.4C: *Der Konformitätsanspruch muss mit der erweiterten Komponentendefinition konsistent sein.*

10.4.1.3.5 Workunit APE_CCL.1-4

Der Evaluator **muss** den Konformitätsanspruch nach ISO/IEC 15408 mit ISO/IEC 15408-2 **untersuchen**, um festzustellen, dass er gegenüber der erweiterten Komponentendefinition konsistent ist.

Wenn der Konformitätsanspruch nach ISO/IEC 15408 ISO/IEC 15408-2-konform enthält, stellt der Evaluator fest, dass die erweiterte Komponentendefinition keine Funktionskomponenten definiert.

Wenn der Konformitätsanspruch nach ISO/IEC 15408 ISO/IEC 15408-2-erweitert enthält, stellt der Evaluator fest, dass die erweiterte Komponentendefinition mindestens eine erweiterte Funktionskomponente definiert.

10.4.1.3.6 Workunit APE_CCL.1-5

Der Evaluator **muss** den Konformitätsanspruch nach ISO/IEC 15408 mit ISO/IEC 15408-3:2022 **untersuchen**, um festzustellen, dass er gegenüber der erweiterten Komponentendefinition konsistent ist.

Wenn der Konformitätsanspruch nach ISO/IEC 15408 ISO/IEC 15408-3:2022-konform enthält, stellt der Evaluator fest, dass die erweiterte Komponentendefinition keine Vertrauenswürdigkeitskomponenten definiert.

Wenn der Konformitätsanspruch nach ISO/IEC 15408 ISO/IEC 15408-3:2022-erweitert enthält, stellt der Evaluator fest, dass die erweiterte Komponentendefinition mindestens eine erweiterte Vertrauenswürdigkeitskomponente definiert.

ISO/IEC 15408-3:2022 APE_CCL.1.5C: *Der Konformitätsanspruch muss alle PPs und Pakete identifizieren, mit denen das PP Konformität beansprucht.*

10.4.1.3.7 Workunit APE_CCL.1-6

Der Evaluator **muss prüfen**, ob der Konformitätsanspruch einen PP-Anspruch enthält, der alle PPs identifiziert, mit denen das PP Konformität beansprucht.

Wenn das PP nicht die Konformität mit einem anderen PP beansprucht, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass alle empfohlenen PPs eindeutig identifiziert werden (z. B. durch Titel und Versionsnummer oder durch die in der Einführung dieses PPs enthaltene Identifizierung).

Der Evaluator wird daran erinnert, dass Ansprüche auf eine teilweise Konformität mit einem PP nicht zulässig sind.

Wenn das PP vom genauen Konformitätstyp ist, stellt der Evaluator fest, dass das PP keine Konformität mit anderen PP beansprucht. Wenn das PP nicht vom genauen Konformitätstyp ist, stellt der Evaluator fest, dass alle PP, deren Konformität beansprucht wird, in ihrer Konformitätserklärung keine genaue Konformität verlangen.

10.4.1.3.8 Workunit APE_CCL.1-7

Der Evaluator **muss** für jedes identifizierte Funktionspaket **prüfen**, ob die Paketdefinition vollständig ist.

Wenn das PP nicht die Konformität mit einem Funktionspaket beansprucht, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator bestimmt, dass die Paketdefinition mit den Anforderungen von ISO/IEC 15408-1:2022, Abschnitt 9 „Pakete“, übereinstimmt, indem er prüft, ob das Funktionspaket Folgendes umfasst:

- a) eine Identifizierung des Funktionspakets, die einen eindeutigen Namen, eine Version, ein Datum, einen Antragsteller und die Ausgabe von ISO/IEC 15408 angibt;
- b) eine Übersicht über das Funktionspaket, die eine Beschreibung der Sicherheitsfunktionalität enthält;
- c) eine Komponentenbegründung für die Auswahl der funktionalen Komponenten/Anforderungen, die im Paket enthalten sind;
- d) wenn das Paket eine SPD festlegt, dann:
 - i) enthält das Paket eine Begründung für die Sicherheitsanforderungen;
 - ii) enthält das Paket eine Begründung für die Sicherheitszielsetzungen, ob Sicherheitszielsetzungen für die Umgebung festgelegt sind;
 - iii) wenn es sich bei dem Paket um ein Paket mit direkter Begründung handelt, sind keine Sicherheitszielsetzungen für den TOE festgelegt, und die Begründung für die Sicherheitsanforderungen wird direkt der SPD zugeordnet;
 - iv) wenn das Paket kein direktes Begründungspaket ist, dann werden Sicherheitszielsetzungen für den TOE festgelegt, die Begründung für die Sicherheitszielsetzungen deckt die Ziele in Bezug auf die SPD ab, und die Begründung für die Sicherheitsanforderungen bildet die Anforderungen auf die Sicherheitszielsetzungen ab;
- e) eine oder mehrere Sicherheitskomponenten oder -anforderungen (die funktionalen Paket-SFR);
- f) wenn erweiterte Komponenten festgelegt wurden, enthält das Funktionspaket eine erweiterte Komponentendefinition.

10.4.1.3.9 Workunit APE_CCL.1-8

Der Evaluator **muss** für jedes identifizierte Sicherheitspaket **prüfen**, ob die Paketdefinition vollständig ist. Wenn das PP nicht die Konformität mit einem Sicherheitspaket beansprucht, ist diese Workunit nicht anwendbar und gilt daher als erfüllt. Wenn das Sicherheitspaket auf eines der in ISO/IEC 15408-5:2022 enthaltenen Sicherheitspakete verweist, gilt auch diese Workunit als erfüllt. Der Evaluator bestimmt, dass die Paketdefinition mit den Anforderungen von ISO/IEC 15408-1:2022, Abschnitt 9 „Pakete“, übereinstimmt, indem er prüft, ob das Sicherheitspaket Folgendes umfasst:

- a) eine Identifizierung des Sicherheitspakets, die einen eindeutigen Namen, eine Version, ein Datum, einen Antragsteller und die Ausgabe von ISO/IEC 15408 angibt;
- b) eine Übersicht über das Sicherheitspaket, die eine Beschreibung der Sicherheitsfunktionalität enthält;
- c) eine oder mehrere Sicherheitskomponenten oder -anforderungen (die SAR für das Sicherheitspaket) aus ISO/IEC 15408-3, erweiterte Vertrauenswürdigkeitskomponenten oder eine Kombination aus beidem;
- d) ein Sicherheitspaket darf weder eine SPD noch Sicherheitszielsetzungen enthalten;
- e) wenn erweiterte Komponenten festgelegt wurden, enthält das Sicherheitspaket eine erweiterte Komponentendefinition;
- f) eine Begründung für die Sicherheitsanforderungen, die eine Begründung für die Auswahl der im Paket enthaltenen Sicherheitskomponenten/Vertrauenswürdigkeitsanforderungen enthält.

ISO/IEC 15408-3:2022 APE_CCL.1.6C: *Der Konformitätsanspruch muss jede Konformität des PP mit einem Funktionspaket als eine der folgenden beschreiben: Paket-konform, Paket-ergänzt oder Paket-angepasst.*

10.4.1.3.10 Workunit APE_CCL.1-9

Der Evaluator **muss prüfen**, ob der Konformitätsanspruch für jedes identifizierte Funktionspaket die Konformität mit diesem Paket als Paket-konform, Paket-ergänzt oder Paket-angepasst angibt. Wenn das PP nicht die Konformität mit einem Funktionspaket beansprucht, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Wenn der Anspruch auf Paketkonformität Paket-konform ist, stellt der Evaluator fest, dass alle im Paket enthaltenen Annahmen, Bedrohungen, OSP, Sicherheitszielsetzungen und SFR in identischer Form im PP enthalten sind (nachdem Iteration, Verfeinerung, Zuweisungen und eine Auswahl aus dem Paket entsprechend den Anforderungen des PP vervollständigt wurden).

Wenn der Anspruch auf Paketkonformität Paket-ergänzt ist, stellt der Evaluator fest, dass alle im Paket enthaltenen Annahmen, Bedrohungen, OSP, Sicherheitszielsetzungen und SFR in identischer Form im PP enthalten sind (nachdem Iteration, Verfeinerung, Zuweisungen und eine Auswahl aus dem Paket entsprechend den Anforderungen des PP vervollständigt wurden) mit der Ausnahme, dass die PP mindestens eine zusätzliche SFR oder eine SFR haben muss, die hierarchisch höher ist als eine SFR im Funktionspaket.

Wenn der Anspruch auf Paketkonformität Paket-angepasst ist, stellt der Evaluator fest, dass alle im Paket enthaltenen Annahmen, Bedrohungen, OSP, Sicherheitszielsetzungen und SFR in identischer Form im PP enthalten sind (nachdem Iteration, Verfeinerung, Zuweisungen und eine Auswahl aus dem Paket entsprechend den Anforderungen des PP vervollständigt wurden) mit der Ausnahme, dass das PP zusätzliche Auswahlwerte für mindestens eine der SFR im Paket enthält und auch eine oder mehrere SFR haben kann, die hierarchisch höher sind als eine SFR im Funktionspaket.

ISO/IEC 15408-3:2022 APE_CCL.1.7C: *Der Konformitätsanspruch muss jede Konformität des PP mit einem Sicherheitspaket entweder als Paket-konform oder als Paket-ergänzt beschreiben.*

10.4.1.3.11 Workunit APE_CCL.1-10

Der Evaluator **muss prüfen**, ob der Konformitätsanspruch für jedes identifizierte Sicherheitspaket einen Anspruch auf Konformität mit diesem Paket als Paket-konform oder Paket-ergänzt angibt.

Wenn der Anspruch auf Paketkonformität Paket-konform ist, stellt der Evaluator fest, dass das PP alle im Paket enthaltenen SARs, aber keine zusätzlichen SARs enthält.

Wenn der Anspruch auf Paketkonformität Paket-ergänzt ist, stellt der Evaluator fest, dass das PP alle im Paket enthaltenen SARs und mindestens eine zusätzliche SAR oder mindestens eine SAR, die hierarchisch zu einer SAR im Paket angeordnet ist, enthält.

ISO/IEC 15408-3:2022 APE_CCL.1.8C: *Der Konformitätsanspruch muss jede Konformität des PP mit einem anderen PP als PP-konform beschreiben.*

10.4.1.3.12 Workunit APE_CCL.1-11

Der Evaluator **muss prüfen**, ob das PP, wenn es Konformität mit einem anderen PP beansprucht, als PP-konform beschrieben ist.

Wenn das PP nicht die Konformität mit einem anderen PP beansprucht, gilt diese Workunit als erfüllt.

ISO/IEC 15408-3:2022 APE_CCL.1.9C: *Die Begründung für den Konformitätsanspruch muss nachweisen, dass der TOE-Typ mit dem TOE-Typ in den PP konsistent ist, für die Konformität beansprucht wird.*

10.4.1.3.13 Workunit APE_CCL.1-12

Der Evaluator **muss** die Begründung für den Konformitätsanspruch **untersuchen**, um festzustellen, dass der TOE-Typ mit allen TOE-Typen der PP konsistent ist.

Wenn das PP nicht die Konformität mit einem anderen PP beansprucht, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Die Beziehung zwischen den Typen kann einfach sein: ein PP für eine Firewall, das Konformität mit einem anderen PP für eine Firewall beansprucht, oder komplexer: ein PP für eine Chipkarte, das gleichzeitig Konformität mit einer Menge anderer PP beansprucht: ein PP für die integrierte Schaltung, ein PP für das Betriebssystem einer Chipkarte und zwei PP für zwei Anwendungen auf der Chipkarte.

ISO/IEC 15408-3:2022 APE_CCL.1.10C: *Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zur Sicherheitsproblemdefinition mit der Aussage zur Sicherheitsproblemdefinition in den PP und allen Funktionspaketen konsistent ist, für die Konformität beansprucht wird.*

10.4.1.3.14 Workunit APE_CCL.1-13

Der Evaluator **muss** die Begründung für den Konformitätsanspruch **untersuchen**, um festzustellen, dass sie die Konsistenz der Aussagen der Sicherheitsproblemdefinition gegenüber den Aussagen der Sicherheitsproblemdefinition in den PPs und den Funktionspaketen, für die Konformität beansprucht wird, unter Berücksichtigung der Konformitätserklärung der PPs nachweist, mit denen Konformität beansprucht wird.

Wenn das zu evaluierende PP nicht die Konformität mit allen PP oder Funktionspaketen beansprucht, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Wenn der Konformitätsanspruch Funktionspakete enthält, bestimmt der Evaluator, dass die Definition des Sicherheitsproblems des zu evaluierenden PP aus allen Annahmen, Bedrohungen und OSP aller Funktionspakete besteht.

Genaue, strikte und nachweisbare Konformität sind die in ISO/IEC 15408-1 definierten Begriffe.

Wenn Pakete verwendet werden, gelten die in den folgenden Abschnitten definierten Regeln zur strikten und nachweisbaren Konformität auch für die den Paketen entnommenen SPD-Beschreibungen.

Da eine PP, die in ihrer Konformitätserklärung strikte oder nachweisbare Konformität festlegt, nur Konformität mit einer anderen PP beanspruchen kann, deren Konformitätserklärung strikte oder nachweisbare Konformität verlangt, sind dies die einzigen Fälle, die in den folgenden Abschnitten behandelt werden. Wenn eine strikte Konformität durch das PP, mit dem Konformität beansprucht wird, gefordert wird, ist keine Begründung für den Konformitätsanspruch erforderlich. Stattdessen bestimmt der Evaluator, ob:

- a) die Bedrohungen in dem zu evaluierenden PP eine Obermenge der Bedrohungen im PP sind, mit dem Konformität beansprucht wird, oder mit diesen identisch sind;
- b) die OSPs in dem zu evaluierenden PP eine Obermenge der OSPs im PP sind, mit dem Konformität beansprucht wird, oder mit diesen identisch sind;
- c) die Annahmen im PP, das Konformität beansprucht, mit den Annahmen im PP, mit dem Konformität beansprucht wird, identisch sind, wobei es zwei mögliche Ausnahmen gibt, die in den folgenden beiden Aufzählungspunkten beschrieben werden:
 - eine Annahme (oder ein Teil einer Annahme) aus dem PP, mit dem Konformität beansprucht wird, weggelassen werden kann, wenn alle Sicherheitszielsetzungen für die Betriebsumgebung, die diese Annahme (oder einen Teil einer Annahme) betreffen, durch Sicherheitszielsetzungen für den TOE ersetzt werden;

- eine Annahme zu der Annahmen hinzugefügt werden kann, die im PP definiert werden, mit dem Konformität beansprucht wird, wenn eine Begründung gegeben wird, warum die neue Annahme weder eine Bedrohung (oder einen Teil einer Bedrohung) abschwächt, die/der durch Sicherheitszielsetzungen für den TOE im PP, mit dem Konformität beansprucht wird, angesprochen werden soll, noch eine OSP (oder einen Teil einer OSP) erfüllt, die/der durch Sicherheitszielsetzungen für den TOE im PP, mit dem Konformität beansprucht wird, angesprochen werden soll.

Die folgende Erörterung liefert die Motivation und Beispiele für Fälle, in denen ein PP Annahmen aus einem anderen PP, mit dem Konformität beansprucht wird, weglässt oder neue Annahmen hinzufügt:

- Beispiel für das Weglassen einer Annahme: Ein PP, mit dem Konformität beansprucht wird, kann eine Annahme enthalten, die besagt, dass die Betriebsumgebung eine unbefugte Änderung oder das Abfangen von Daten, die an eine externe Schnittstelle des TOE gesendet werden, verhindert. Dies kann der Fall sein, wenn der TOE Daten im Klartext und ohne Integritätsschutz an dieser Schnittstelle akzeptiert und davon ausgegangen wird, dass er sich in einer sicheren Betriebsumgebung befindet, die Angreifern den Zugriff auf diese Daten verwehrt. Die Annahme wird dann im PP, mit dem Konformität beansprucht wird, auf eine Zielsetzung für die Betriebsumgebung abgebildet, die angibt, dass die an dieser Schnittstelle ausgetauschten Daten durch geeignete Maßnahmen in der Betriebsumgebung geschützt sind. Wenn ein PP, das dieses PP beansprucht, einen sichereren TOE definiert, der eine zusätzliche Sicherheitszielsetzung hat, die angibt, dass der TOE selbst diese Daten schützt, z. B. durch Bereitstellung eines sicheren Kanals für die Verschlüsselung und den Integritätsschutz aller über diese Schnittstelle übertragenen Daten, können die entsprechende Zielsetzung und die Annahme für die Betriebsumgebung beim PP, das Konformität beansprucht, weggelassen werden. Dies wird auch als Neuzuweisung der Zielsetzung bezeichnet, da die Zielsetzung aus der Betriebsumgebung erneut dem TOE zugewiesen wird. Es ist zu beachten, dass dieser TOE in einer Betriebsumgebung, die die weggelassene Annahme erfüllt, immer noch sicher ist und daher immer noch das PP erfüllt, mit dem Konformität beansprucht wird.
- Beispiel für das Hinzufügen einer Annahme: In diesem Beispiel soll das PP, mit dem Konformität beansprucht wird, die Anforderungen an einen TOE vom Typ „Firewall“ festlegen, und der Autor eines anderen PP möchte die Konformität mit diesem PP für einen TOE beanspruchen, der eine Firewall implementiert, aber zusätzlich die Funktionalität einer Komponente für ein Virtuelles Privates Netzwerk (VPN) bietet. Für die VPN-Funktionalität benötigt der TOE kryptographische Schlüssel, und diese Schlüssel müssen unter Umständen auch von der Betriebsumgebung sicher gehandhabt werden (z. B. wenn symmetrische Schlüssel zur Sicherung der Netzwerkverbindung verwendet werden und daher auf sichere Weise anderen Komponenten im Netzwerk zur Verfügung gestellt werden müssen). In diesem Fall ist es akzeptabel, die Annahme hinzuzufügen, dass die vom VPN verwendeten kryptographischen Schlüssel von der Betriebsumgebung sicher gehandhabt werden. Diese Annahme bezieht sich nicht auf Bedrohungen oder OSPs des PP, mit dem Konformität beansprucht wird, und erfüllt daher die oben genannten Bedingungen.
- Gegenbeispiel für das Hinzufügen einer Annahme: In einer Variante des ersten Beispiels kann ein PP, mit dem Konformität beansprucht wird, bereits eine Zielsetzung für den TOE enthalten, um einen sicheren Kanal für eine seiner Schnittstellen bereitzustellen, und diese Zielsetzung wird auf die Gefahr einer unbefugten Änderung oder eines unbefugten Lesens der Daten auf dieser Schnittstelle abgebildet. In diesem Fall ist es eindeutig nicht erlaubt, dass ein anderes PP, das dieses PP beansprucht, eine Annahme für die Betriebsumgebung hinzufügt, die davon ausgeht, dass die Betriebsumgebung die Daten auf dieser Schnittstelle vor Veränderung oder unbefugtem Lesen der Daten schützt. Diese Annahme würde eine Bedrohung reduzieren, die durch den TOE angesprochen werden soll. Daher würde ein TOE, der ein PP mit dieser zusätzlichen Annahme erfüllt, nicht mehr automatisch das PP erfüllen, mit dem Konformität beansprucht wird, und dieser Zusatz ist daher nicht zulässig.

- zweites Gegenbeispiel für das Hinzufügen einer Annahme: Im obigen Beispiel eines TOE, der eine Firewall implementiert, wäre es nicht zulässig, eine allgemeine Annahme hinzuzufügen, dass der TOE nur mit vertrauenswürdigen Geräten verbunden ist, da dies offensichtlich wesentliche, für eine Firewall relevante Bedrohungen beseitigen würde (und zwar, dass es nicht vertrauenswürdigen IP-Verkehr gibt, der gefiltert werden muss). Daher wäre dieser Zusatz nicht zulässig.

Wenn durch das PP, mit dem Konformität beansprucht wird, eine nachweisbare Konformität gefordert wird, untersucht der Evaluator die Begründung für den Konformitätsanspruch, um festzustellen, ob sie nachweist, dass die Aussage der Sicherheitsproblemdefinition des zu evaluierenden PP gleichwertig oder restriktiver ist als die Aussage der Sicherheitsproblemdefinition im PP, mit dem Konformität beansprucht wird.

Dazu muss die Begründung des Konformitätsanspruchs nachweisen, dass die Sicherheitsproblemdefinition im PP, das Konformität beansprucht, gleichwertig (oder restriktiver) ist als die Sicherheitsproblemdefinition im PP, mit dem Konformität beansprucht wird. Das bedeutet, dass

- alle TOEs, die der Sicherheitsproblemdefinition im PP, das Konformität beansprucht, entsprechen würden, auch der Sicherheitsproblemdefinition im PP, mit dem Konformität beansprucht wird, entsprechen. Dies kann auch indirekt durch den Nachweis aufgezeigt werden, dass jedes Ereignis, das eine Bedrohung realisiert, die im PP definiert wird, mit dem Konformität beansprucht wird, oder gegen eine OSP verstößt, die im PP definiert ist, mit dem Konformität beansprucht wird, auch eine Bedrohung realisieren würde, die im PP angegeben wird, das Konformität beansprucht, oder gegen eine OSP verstoßen würde, die im PP definiert wird, das Konformität beansprucht. Es ist zu beachten, dass die Erfüllung einer OSP, die im PP angegeben wird, das Konformität beansprucht, eine Bedrohung abwenden kann, die im PP angegeben wird, mit dem Konformität beansprucht wird, oder dass die Abwendung einer Bedrohung, die im PP angegeben wird, das Konformität beansprucht, eine OSP erfüllen kann, die im PP angegeben wird, mit dem Konformität beansprucht wird, so dass Bedrohungen und OSPs sich gegenseitig ersetzen können,
- alle Betriebsumgebungen, die der Sicherheitsproblemdefinition im PP, mit dem Konformität beansprucht wird, entsprechen würden, auch der Sicherheitsproblemdefinition im PP, das Konformität beansprucht, entsprechen würden (mit einer Ausnahme im nächsten Aufzählungspunkt),
- neben einer Menge Annahmen im PP, das Konformität beansprucht, die erforderlich sind, um die Konformität mit der SPD des PP, mit dem Konformität beansprucht wird, nachzuweisen, kann ein PP, das Konformität beansprucht, weitere Annahmen festlegen, jedoch nur, wenn diese zusätzlichen Annahmen unabhängig von der Sicherheitsproblemdefinition sind, wie sie im PP, mit dem Konformität beansprucht wird, definiert ist, und diese nicht beeinflussen. Genauer gesagt gibt es im PP, das Konformität beansprucht, keine Annahmen, die Bedrohungen für den TOE ausschließen, denen der TOE nach dem PP, mit dem Konformität beansprucht wird, entgegenwirken muss. Ebenso gibt es im PP, das Konformität beansprucht, keine Annahmen, die Aspekte einer OSP realisieren, die im PP, mit dem Konformität beansprucht wird, angegeben sind und die vom TOE nach dem PP, für das Konformität beansprucht wird, erfüllt werden sollen.

ISO/IEC 15408-3:2022 APE_CCL.1.11C: *Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zu den Sicherheitszielsetzungen mit der Aussage zu den Sicherheitszielsetzungen in den PPs und allen Funktionspaketen konsistent ist, für die Konformität beansprucht wird.*

10.4.1.3.15 Workunit APE_CCL.1-14

Der Evaluator **muss** die Begründung für den Konformitätsanspruch **untersuchen**, um festzustellen, dass die Aussage der Sicherheitszielsetzungen gegenüber der Aussage der Sicherheitszielsetzungen in den PP und Funktionspaketen, mit denen Konformität beansprucht wird, unter Berücksichtigung der Konformitäts-erklärung der PP, mit denen Konformität beansprucht wird, konsistent ist.

Wenn das PP nicht die Konformität mit einem anderen PP oder mit Funktionspaketen beansprucht, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Wenn die Konformität mit allen Funktionspaketen beansprucht wird, stellt der Evaluator fest, dass die Sicherheitszielsetzungen des zu evaluierenden PP alle Sicherheitszielsetzungen der gesamten Funktionspakete einschließen, mit denen Konformität beansprucht wird.

Wenn Pakete verwendet werden, gelten die in den folgenden Absätzen definierten Regeln zur strikten und nachweislichen Konformität auch für die den Paketen entnommenen Sicherheitszielsetzungen.

Da eine PP nur Konformität mit einem anderen PP beanspruchen kann, dessen Konformitätserklärung strikte oder nachweisliche Konformität verlangt, sind dies die einzigen Fälle, die in den folgenden Absätzen behandelt werden. Wenn eine strikte Konformität durch das PP, mit dem Konformität beansprucht wird, gefordert wird, ist keine Begründung für den Konformitätsanspruch erforderlich. Stattdessen bestimmt der Evaluator, ob:

- a) das zu evaluierende PP alle Sicherheitszielsetzungen für den TOE des PP, mit dem Konformität beansprucht wird, enthält. Es ist zu beachten, dass es zulässig ist für das zu evaluierende PP, zusätzliche Sicherheitszielsetzungen für den TOE aufzuweisen;
- b) die Sicherheitszielsetzungen für die Betriebsumgebung im PP, das Konformität beansprucht, identisch mit den Sicherheitszielsetzungen für die Betriebsumgebung im PP sind, mit dem Konformität beansprucht wird, mit zwei möglichen Ausnahmen, die in den folgenden zwei Aufzählungspunkten beschrieben werden;
- c) eine Sicherheitszielsetzung für die Betriebsumgebung (oder ein Teil einer solchen Sicherheitszielsetzung) aus dem PP, mit dem Konformität beansprucht wird, kann durch dieselbe (denselben Teil der) für den TOE angegebene(n) Sicherheitszielsetzung ersetzt werden;
- d) eine Sicherheitszielsetzung für die Betriebsumgebung kann zu den Zielsetzungen hinzugefügt werden, die im PP definiert werden, mit dem Konformität beansprucht wird, wenn eine Begründung gegeben wird, warum die neue Zielsetzung weder eine Bedrohung (oder einen Teil einer Bedrohung) abschwächt, die durch Sicherheitszielsetzungen für den TOE im PP, mit dem die Konformität beansprucht wird, angesprochen werden soll, noch eine OSP (oder einen Teil einer OSP) erfüllt, die/der durch Sicherheitszielsetzungen für den TOE im PP, mit dem Konformität beansprucht wird, angesprochen werden soll.

Bei der Untersuchung eines PP, das ein anderes PP beansprucht, das Sicherheitszielsetzungen für die Betriebsumgebung aus dem PP, mit dem Konformität beansprucht wird, weglässt oder neue Sicherheitszielsetzungen für die Betriebsumgebung hinzufügt, muss der Evaluator genau festlegen, ob die oben genannten Bedingungen erfüllt sind. Die Beispiele, die für die Annahmen in der vorangegangenen Workunit angegeben wurden, gelten auch hier.

Wenn durch das PP, mit dem Konformität beansprucht wird, eine nachweisbare Konformität gefordert wird, untersucht der Evaluator die Begründung für den Konformitätsanspruch, um festzustellen, ob sie nachweist, dass die Aussage der Sicherheitszielsetzungen des zu evaluierenden PP gleichwertig oder restriktiver ist als die Aussage der Sicherheitszielsetzungen im PP, mit dem Konformität beansprucht wird.

Dazu muss die Begründung des Konformitätsanspruchs nachweisen, dass die Sicherheitszielsetzungen im PP, mit dem Konformität beansprucht wird, gleichwertig (oder restriktiver) ist als die Sicherheitszielsetzungen im PP, mit dem Konformität beansprucht wird. Das bedeutet, dass:

- a) alle TOEs, die die Sicherheitszielsetzungen für den TOE im PP, das Konformität beansprucht, erfüllen würden, auch die Sicherheitszielsetzungen für den TOE im PP, mit dem Konformität beansprucht wird, erfüllen;
- b) alle Betriebsumgebungen, die die Sicherheitszielsetzungen für die Betriebsumgebung im PP, mit dem Konformität beansprucht wird, erfüllen würden, auch die Sicherheitszielsetzungen für die Betriebsumgebung im PP, das Konformität beansprucht, erfüllen würden (mit einer Ausnahme im nächsten Aufzählungspunkt);

- c) neben einer Menge Sicherheitszielsetzungen für die Betriebsumgebung im PP, das Konformität beansprucht, die zum Nachweis der Konformität mit der Menge Sicherheitszielsetzungen verwendet werden, die im PP definiert sind, mit dem Konformität beansprucht wird, kann ein PP, das Konformität beansprucht, weitere Sicherheitszielsetzungen für die Betriebsumgebung festlegen, jedoch nur dann, wenn diese Sicherheitszielsetzungen weder die ursprüngliche Menge Sicherheitszielsetzungen für den TOE noch die Sicherheitszielsetzungen für die Betriebsumgebung, wie sie im PP, mit dem Konformität beansprucht wird, definiert sind, beeinflussen.

ISO/IEC 15408-3:2022 APE_CCL.1.12C: *Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zu den Sicherheitsanforderungen mit der Aussage zu den Sicherheitsanforderungen in den PPs und allen Funktionspaketen konsistent ist, für die Konformität beansprucht wird.*

10.4.1.3.16 Workunit APE_CCL.1-15

Der Evaluator **muss** das PP **untersuchen**, um festzustellen, dass die Aussage der Sicherheitsanforderungen gegenüber der Aussage aller Sicherheitsanforderungen in den PP und jeglichen Funktionspaketen, mit denen Konformität beansprucht wird, unter Berücksichtigung der Konformitätserklärungen der PP, mit denen Konformität beansprucht wird, konsistent ist.

Wenn das PP nicht die Konformität mit einem anderen PP oder mit Funktionspaketen beansprucht, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Wenn die Konformität mit allen Funktionspaketen beansprucht wird, stellt der Evaluator fest, dass die SFR des zu evaluierenden PP alle SFR (oder hierarchische SFR) aller Funktionspakete einschließen, mit denen Konformität beansprucht wird.

Wenn Pakete verwendet werden, gelten die in den folgenden Absätzen definierten Regeln zur strikten und nachweislichen Konformität auch für die den Paketen entnommenen SFR.

Da eine PP nur Konformität mit einem anderen PP beanspruchen kann, dessen Konformitätserklärung strikte oder nachweisliche Konformität verlangt, sind dies die einzigen Fälle, die in den folgenden Absätzen behandelt werden.

Wenn eine strikte Konformität durch das PP, mit dem Konformität beansprucht wird, gefordert wird, ist keine Begründung für den Konformitätsanspruch erforderlich. Stattdessen bestimmt der Evaluator, ob die Aussage der Sicherheitsanforderungen in dem zu evaluierenden PP eine Obermenge der Aussage der Sicherheitsanforderungen in dem PP ist, mit dem Konformität (bei strikter Konformität) beansprucht wird, oder ob sie mit dieser identisch ist.

Wenn durch das PP, mit dem Konformität beansprucht wird, eine nachweisbare Konformität gefordert wird, untersucht der Evaluator die Begründung für den Konformitätsanspruch, um festzustellen, ob sie nachweist, dass die Aussage der Sicherheitsanforderungen des zu evaluierenden PP gleichwertig oder restriktiver ist als die Aussage der Sicherheitsanforderungen in dem PP, mit dem Konformität beansprucht wird.

Bei

- SFRs: Die Begründung für die Konformität in dem PP, mit dem Konformität beansprucht wird, muss nachweisen, dass die Gesamtanforderungen, die von den SFRs in dem PP definiert sind, mit dem Konformität beansprucht wird, gleichwertig (oder restriktiver) sind als die Gesamtanforderungen, die von den SFRs in dem PP definiert sind, mit dem Konformität beansprucht wird. Dies bedeutet, dass alle TOEs, die die Anforderungen erfüllen würden, die durch die Menge aller SFRs im PP definiert sind, mit dem Konformität beansprucht wird, auch die Anforderungen erfüllen würden, die durch die Menge aller SFRs im PP definiert sind, mit dem Konformität beansprucht wird.

- SARs: Das PP, das die Konformität beansprucht, muss alle SARs im PP enthalten, mit dem Konformität beansprucht wird, kann aber zusätzliche SARs beanspruchen oder die SARs durch hierarchisch stärkere SARs ersetzen. Die Vervollständigung der Operationen in dem PP, das Konformität beansprucht, muss konsistent gegenüber der Vervollständigung in dem PP sein, mit dem Konformität beansprucht wird; entweder wird in dem PP, das Konformität beansprucht, die gleiche Vervollständigung verwendet wie in dem PP, mit dem Konformität beansprucht wird, oder eine Vervollständigung, die für eine restriktivere SAR sorgt (es gelten die Regeln zur Präzisierung).

ISO/IEC 15408-3:2022 APE_CCL.1.13C: *Die Konformitätserklärung muss die geforderte Konformität aller PPs/STs mit dem PP als genaue PP-Konformität, strikte PP-Konformität oder nachweisliche PP-Konformität beschreiben.*

10.4.1.3.17 Workunit APE_CCL.1-16

Der Evaluator **muss prüfen**, ob die PP-Konformitätserklärung einen Anspruch der genauen PP-, strikten PP- oder nachweislichen PP-Konformität angibt.

ISO/IEC 15408-3:2022 APE_CCL.1.14C: *Für eine genaue Konformitäts-PP muss die Konformitätserklärung eine Zulässigkeitsaussage enthalten, die die Menge des PP (falls vorhanden) identifiziert, für den in Kombination mit dem zu evaluierenden PP eine genaue Konformität beansprucht werden kann.*

10.4.1.3.18 Workunit APE_CCL.1-17

Der Evaluator **muss** die Konformitätserklärung **prüfen**, um festzustellen, ob sie eine Zulässigkeitsaussage enthält, die die Reihe der PP auflistet, für die in Kombination mit dem zu evaluierenden PP ein genauer Konformitätsanspruch (in einer ST oder PP-Konfiguration) zulässig ist.

Wenn das PP in seiner Konformitätserklärung keine genaue Konformität verlangt, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Wenn das PP in Kombination mit anderen PP keine Ansprüche auf eine genaue Konformität mit ihm zulässt, ist keine Liste von PP erforderlich, und diese Workunit gilt daher als erfüllt.

Die Verwendung der Zulässigkeitsaussage ist eine Frage der Politik und wird hier nicht behandelt. Außer der Feststellung, dass die Liste vorhanden ist, gibt es für den Evaluator keine weiteren Aktionen.

ISO/IEC 15408-3:2022 APE_CCL.1.15C: *Für ein genaues Konformitäts-PP muss die Konformitätserklärung eine Zulässigkeitsaussage enthalten, in der die Reihe von PP-Modulen (falls vorhanden) angegeben ist, die mit dem zu evaluierenden PP in einer PP-Konfiguration verwendet werden dürfen.*

10.4.1.3.19 Workunit APE_CCL.1-18

Der Evaluator **muss** die Konformitätserklärung **prüfen**, um festzustellen, ob sie eine Zulässigkeitsaussage enthält, die die Reihe der PP-Module auflistet, die in Kombination mit dem zu evaluierenden PP in einer PP-Konfiguration vorhanden sein können, für die eine genaue Konformität erforderlich ist.

Wenn das PP in seiner Konformitätserklärung keine genaue Konformität verlangt, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Wenn das PP in Kombination mit PP-Modulen keine Ansprüche auf eine genaue Konformität mit ihm zulässt, ist keine Liste von PP-Modulen erforderlich, und diese Workunit gilt daher als erfüllt.

Die Verwendung der Zulässigkeitsaussage ist eine Frage der Politik und wird hier nicht behandelt. Außer der Feststellung, dass die Liste vorhanden ist, gibt es für den Evaluator keine weiteren Aktionen.

ISO/IEC 15408-3:2022 APE_CCL.1.16C: *Die Konformitätserklärung muss den Satz von abgeleiteten Evaluierungsverfahren und Evaluierungsaufgaben (falls vorhanden) angeben, die mit dem zu evaluierenden PP verwendet werden müssen. Diese Liste muss Folgendes enthalten:*

- *alle Evaluierungsverfahren und Evaluierungsaufgaben, die für das zu evaluierende PP festgelegt sind;*
- *alle Evaluierungsverfahren und Evaluierungsaufgaben, die in Konformitätserklärungen der PP festgelegt sind, mit denen Konformität des zu evaluierenden PP beansprucht wird;*
- *alle Evaluierungsverfahren und Evaluierungsaufgaben, die in den Abschnitten über die Sicherheitsanforderungen der Pakete festgelegt sind, mit denen Konformität des zu evaluierenden PP beansprucht wird.*

10.4.1.3.20 Workunit APE_CCL.1-19

Der Evaluator **muss** die Konformitätserklärung des zu evaluierenden PP **prüfen**, um Folgendes festzustellen:

- a) wenn abgeleitete Evaluierungsverfahren und Evaluierungsaufgaben von anderen Punkten gefordert werden, mit denen das PP Konformität beansprucht, werden diese in dem zu evaluierenden PP identifiziert, zusammen mit allen abgeleiteten Evaluierungsverfahren und Evaluierungsaufgaben, die das PP selbst fordert;
- b) die Liste der abgeleiteten Evaluierungsverfahren und Evaluierungsaufgaben hinreichend strukturiert und detailliert ist, um jedes Mitglied der Liste eindeutig identifizieren und lokalisieren zu können;
- c) wenn es eine Überschneidung im Anwendungsbereich der identifizierten Evaluierungsverfahren und Evaluierungsaufgaben gibt (d. h. wenn es eine Überschneidung gibt, wie in ISO/IEC 15408-4 beschrieben), dann ist die Begründung für die sich ergebende Menge von Evaluierungsverfahren und Evaluierungsaufgaben auf den TOE anwendbar, wie er von dem zu evaluierenden PP beschrieben wird.

Mit dieser Workunit soll sichergestellt werden, dass bei der Evaluierung eines TOE, der Konformität mit dem zu evaluierenden PP beansprucht, die richtigen Evaluierungsverfahren und Evaluierungsaufgaben verwendet werden können. Das bedeutet, dass die Identifizierung im PP keine einzelnen Evaluierungsaufgaben auflisten muss, wenn diese eindeutig in einem aufgeführten Evaluierungsverfahren enthalten sind. Wenn mehrere Evaluierungsverfahren oder Evaluierungsaufgaben in einem einzigen Dokument enthalten sind, ist es ausreichend, auf das Dokument zu verweisen, vorausgesetzt, dies führt zu einer eindeutigen Identifizierung der Evaluierungsverfahren und Evaluierungsaufgaben, die für das zu evaluierende PP gelten.

BEISPIEL Wenn ein Dokument mehrere verschiedene Evaluierungsverfahren auflistet, die auf unterschiedliche Anwendungsfälle anwendbar sind, dann würde es nicht ausreichen, auf das Dokument zu verweisen: die relevanten Anwendungsfälle müssten ebenfalls identifiziert werden.

10.5 Sicherheitsproblemdefinition (APE_SPD)

10.5.1 Evaluierung der Unteraufgabe (APE_SPD.1)

10.5.1.1 Zielsetzungen

Die Zielsetzung dieser Unteraufgabe besteht darin, festzustellen, ob das Sicherheitsproblem, das durch den TOE und seine Betriebsumgebung angesprochen werden soll, klar definiert ist.

10.5.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist:

- a) das PP.

10.5.1.3 Aktion APE_SPD.1.1E

10.5.1.3.1 Allgemeines

ISO/IEC 15408-3:2022 APE_SPD.1.1C: *Die Sicherheitsproblemdefinition muss die Bedrohungen beschreiben.*

10.5.1.3.2 Workunit APE_SPD.1-1

Der Evaluator **muss prüfen**, ob die Sicherheitsproblemdefinition die Bedrohungen beschreibt.

Wenn alle Sicherheitszielsetzungen nur aus Annahmen und/oder OSPs abgeleitet werden, muss die Aussage der Bedrohungen im PP nicht vorhanden sein. In diesem Fall ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass die Sicherheitsproblemdefinition die Bedrohungen beschreibt, denen der TOE und/oder seine Betriebsumgebung entgegenwirken muss.

Es ist zu beachten, dass bei der Festlegung von optionalen Anforderungen durch das PP möglicherweise damit verbundene Bedrohungen durch diese Workunit abgedeckt werden.

ISO/IEC 15408-3:2022 APE_SPD.1.2C: *Alle Bedrohungen müssen in Bezug auf einen Bedrohungsagenten, einen Vermögenswert und eine unerwünschte Aktion beschrieben werden.*

10.5.1.3.3 Workunit APE_SPD.1-2

Der Evaluator **muss** die Sicherheitsproblemdefinition **untersuchen**, um festzustellen, dass alle Bedrohungen anhand eines Bedrohungsagenten, eines Vermögenswertes und einer unerwünschten Aktion beschrieben werden.

Wenn alle Sicherheitszielsetzungen nur aus Annahmen und OSPs abgeleitet werden, muss die Aussage der Bedrohungen im PP nicht vorhanden sein. In diesem Fall ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Bedrohungsagenten können noch weiter über Aspekte wie Fachkenntnis, Ressource, Möglichkeit und Motivation beschrieben werden.

ISO/IEC 15408-3:2022 APE_SPD.1.3C: *Die Sicherheitsproblemdefinition muss die organisatorischen Sicherheitsrichtlinien (OSPs) beschreiben.*

10.5.1.3.4 Workunit APE_SPD.1-3

Der Evaluator **muss untersuchen**, ob die Sicherheitsproblemdefinition die OSPs beschreibt.

Wenn alle Sicherheitszielsetzungen nur aus Annahmen und/oder Bedrohungen abgeleitet werden, müssen OSPs im PP nicht vorhanden sein. In diesem Fall ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass OSP-Aussagen in Form von Regeln oder Leitlinien gemacht werden, die vom TOE und/oder seiner Betriebsumgebung befolgt werden müssen.

Der Evaluator stellt fest, dass jede OSP ausreichend detailliert erklärt und/oder interpretiert wird, um sie klar verständlich zu machen; eine klare Darstellung der Grundsatzserklärungen ist notwendig, um die Rückverfolgung der Sicherheitszielsetzungen zu ermöglichen.

Es ist zu beachten, dass bei der Festlegung von optionalen Anforderungen durch das PP möglicherweise damit verbundene OSP durch diese Workunit abgedeckt werden.

ISO/IEC 15408-3:2022 APE_SPD.1.4C: *Die Sicherheitsproblemdefinition muss die Annahmen über die Betriebsumgebung des TOE beschreiben.*

10.5.1.3.5 Workunit APE_SPD.1-4

Der Evaluator **muss** die Sicherheitsproblemdefinition **untersuchen**, um festzustellen, dass er die Annahmen über die Betriebsumgebung des TOE beschreibt.

Gibt es keine Annahmen, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass jede Annahme über die Betriebsumgebung des TOE hinreichend detailliert erläutert wird, damit die Verbraucher feststellen können, dass ihre Betriebsumgebung mit der Annahme übereinstimmt. Wenn die Annahmen nicht klar verstanden werden, kann das Endergebnis sein, dass der TOE in einer Betriebsumgebung verwendet wird, in der er nicht in sicherer Weise funktioniert.

10.6 Sicherheitszielsetzungen (APE_OBJ)

10.6.1 Evaluierung der Unteraufgabe (APE_OBJ.1)

10.6.1.1 Zielsetzungen

Die Zielsetzung dieser Unteraufgabe besteht darin, festzustellen, ob die Sicherheitszielsetzungen für die Betriebsumgebung klar definiert sind.

10.6.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist:

a) das PP.

10.6.1.3 Aktion APE_OBJ.1.1E

10.6.1.3.1 Allgemeines

ISO/IEC 15408-3:2022 APE_OBJ.1.1C: *Die Aussage zu den Sicherheitszielsetzungen muss die Sicherheitszielsetzungen für die Betriebsumgebung beschreiben.*

10.6.1.3.2 Workunit APE_OBJ.1-1

Der Evaluator **muss prüfen**, ob die Aussage der Sicherheitszielsetzungen die Sicherheitszielsetzungen für die Betriebsumgebung definiert.

Der Evaluator prüft, ob die Sicherheitszielsetzungen für die Betriebsumgebung festgelegt sind.

ISO/IEC 15408-3:2022 APE_OBJ.1.2C: *Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für die Betriebsumgebung zurückführen zu den Bedrohungen, die durch diese Sicherheitszielsetzung abgewehrt werden, zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden, und zu den Annahmen, die durch diese Sicherheitszielsetzung eingehalten werden.*

10.6.1.3.3 Workunit APE_OBJ.1-2

Der Evaluator **muss prüfen**, ob die Begründung der Sicherheitszielsetzungen die Sicherheitszielsetzungen für die Betriebsumgebung auf Bedrohungen zurückführt, denen diese Sicherheitszielsetzung entgegenwirkt, auf die durch diese Sicherheitszielsetzung durchgesetzten OSPs und auf die durch diese Sicherheitszielsetzung eingehaltenen Annahmen.

Jede Sicherheitszielsetzung für die Betriebsumgebung kann auf Bedrohungen, OSPs, Annahmen oder eine Kombination von Bedrohungen, OSPs und/oder Annahmen zurückführen, sie muss aber auf mindestens eine Bedrohung, OSP oder Annahme zurückführen.

Eine fehlende Rückführung einer Sicherheitszielsetzung für die Betriebsumgebung auf mindestens eine Bedrohung, OSP oder Annahme bedeutet, dass entweder die Begründung der Sicherheitszielsetzungen unvollständig ist, dass die Sicherheitsproblemdefinition unvollständig ist oder dass die Sicherheitszielsetzung für die Betriebsumgebung keinen sinnvollen Zweck hat.

Es gibt keinen vorgeschriebenen Ort, an dem dieses Element der Begründung eingeordnet werden muss: Die entsprechenden Teile können beispielsweise unter jeder Bedrohung, jeder OSP und jeder Annahme eingeordnet werden, um das Sicherheitsargument klarer und leichter lesbar zu machen.

ISO/IEC 15408-3:2022 APE_OBJ.1.3C: *Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen für die Betriebsumgebung alle Annahmen einhalten.*

10.6.1.3.4 Workunit APE_OBJ.1-3

Der Evaluator **muss** die Begründung der Sicherheitszielsetzungen **untersuchen**, um festzustellen, dass sie für jede Annahme für die Betriebsumgebung eine angemessene Begründung dafür enthält, dass die Sicherheitszielsetzungen für die Betriebsumgebung geeignet sind, diese Annahme zu bestätigen.

Wenn keine Sicherheitszielsetzungen für die Betriebsumgebung auf die Annahme zurückführen, wird die Evaluatorenaktion, die sich auf diese Workunit bezieht, mit einer „abgelehnt“ Entscheidung belegt.

Der Evaluator stellt fest, dass die Begründung für eine Annahme über die Betriebsumgebung des TOE zeigt, dass die Sicherheitszielsetzungen ausreichend sind: Wenn alle Sicherheitszielsetzungen für die Betriebsumgebung, die auf diese Annahme zurückführen, erreicht werden, hält die Betriebsumgebung die Annahme aufrecht.

Der Evaluator stellt auch fest, dass jede Sicherheitszielsetzung für die Betriebsumgebung, die auf eine Annahme über die Betriebsumgebung des TOE zurückführt, notwendig ist: Wenn die Sicherheitszielsetzung erreicht ist, trägt sie tatsächlich dazu bei, dass die Betriebsumgebung die Annahme aufrechterhält.

Es ist zu beachten, dass die bloße Auflistung der Sicherheitszielsetzungen für die Betriebsumgebung, die mit jeder Annahme verbunden sind, in der Begründung der Sicherheitszielsetzungen zwar ein Teil einer Begründung sein kann, aber keine Begründung für sich selbst darstellt. Eine beschreibende Begründung ist erforderlich, obwohl diese Begründung in einfachen Fällen so minimal sein kann wie „Sicherheitszielsetzung X hält die Annahme Y direkt aufrecht“.

10.6.2 Evaluierung der Unteraufgabe (APE_OBJ.2)

10.6.2.1 Zielsetzungen

Die Zielsetzung dieser Unteraufgabe besteht darin, festzustellen, ob die Sicherheitszielsetzungen die Sicherheitsproblemdefinition angemessen und vollständig berücksichtigen und ob die Aufteilung dieses Problems zwischen dem TOE und seiner Betriebsumgebung klar definiert ist.

10.6.2.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist:

- a) das PP.