DIN EN ISO/IEC 18045

ICS 35.030

Informationstechnik – Sicherheitstechniken – Methodik für die Bewertung der IT-Sicherheit (ISO/IEC 18045:2008); Deutsche Fassung EN ISO/IEC 18045:2020, nur auf CD-ROM

Information technology –
Security techniques –
Methodology for IT security evaluation (ISO/IEC 18045:2008);
German version EN ISO/IEC 18045:2020, only on CD-ROM

Technologies de l'information –
Techniques de sécurité –
Méthodologie pour l'évaluation de sécurité TI (ISO/IEC 18045:2008);
Version allemande EN ISO/IEC 18045:2020, seulement en CD-ROM

Gesamtumfang 344 Seiten

DIN-Normenausschuss Informationstechnik und Anwendungen (NIA)

AVA Documents Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

Nationales Vorwort

Der Text von ISO/IEC 18045:2008 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 18045:2020 durch das Technische Komitee CEN/TC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN (Deutschland) gehalten wird.

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

Für die in diesem Dokument zitierten Dokumente wird im Folgenden auf die entsprechenden deutschen Dokumente hingewiesen:

ISO/IEC 15408 (all parts) siehe DIN EN ISO/IEC 15408 (alle Teile)

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

Nationaler Anhang NA
(informativ)

Literaturhinweise

DIN EN ISO/IEC 15408 (alle Teile), *Informationstechnik — IT-Sicherheitsverfahren —- Evaluationskriterien für IT-Sicherheit*

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

EUROPÄISCHE NORM

EUROPEAN STANDARD

NORME EUROPÉENNE

EN ISO/IEC 18045

März 2020

ICS 35.030

Deutsche Fassung

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

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

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

Diese Europäische Norm wurde vom CEN am 2. März 2020 angenommen.

Die CEN und CENELEC-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim CEN-CENELEC-Management-Zentrum oder bei jedem CEN und CENELEC-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN und CENELEC-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN- und CENELEC-Mitglieder sind die nationalen Normungsinstitute und elektrotechnischen Komitees von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, der Republik Nordmazedonien, Rumänien, Schweden, der Schweiz, Serbien, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, der Türkei, Ungarn, dem Vereinigten Königreich und Zypern.

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

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

Inhalt

Seite

Europäisches Vorwort 7
Vorwort 8
Rechtliche Hinweise 9
Einleitung 10
1 Anwendungsbereich 11
2 Normative Verweisungen 11
3 Begriffe 11
4 Symbole und Abkürzungen 13
5 Überblick 13
5.1 Gliederung dieser Internationalen Norm 13
6 Typographische Konventionen 14
6.1 Terminologie 14
6.2 Verbgebrauch 14
6.3 Allgemeine Evaluierungsleitlinien 14
6.4 Beziehung zwischen den Strukturen von ISO/IEC 15408 und ISO/IEC 18045 14
7 Evaluierungsprozess und damit verbundene Arbeitsaufgaben 15
7.1 Einleitung 15
7.2 Überblick über den Evaluierungsprozess 16
7.2.1 Zielsetzungen 16
7.2.2 Verantwortlichkeiten der Rollen 16
7.2.3 Beziehung der Rollen 16
7.2.4 Allgemeines Evaluierungsmodell 16
7.2.5 Evaluatoren-Entscheidungen 17
7.3 Eingabearbeitsaufgabe der Evaluierung 19
7.3.1 Zielsetzungen 19
7.3.2 Anwendungshinweise 19
7.3.3 Management der Teilarbeitsaufgabe der Evaluationsnachweise 20
7.4 Evaluierungsunteraufgaben 20
7.5 Ausgabearbeitsaufgabe der Evaluierung 20
7.5.1 Zielsetzungen 20
7.5.2 Management der Evaluierungsausgaben 21
7.5.3 Anwendungshinweise 21
7.5.4 OR-Teilarbeitsaufgabe schreiben 21
7.5.5 ETR-Teilarbeitsaufgabe schreiben 22
8 Klasse APE: Evaluierung des Schutzprofils 27
8.1 Einleitung 27
8.2 Anwendungshinweise 28
8.2.1 Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs 28
8.3 PP-Einleitung (APE_INT) 28
8.3.1 Evaluierung der Unteraufgabe (APE_INT.1) 28
8.4 Konformitätsansprüche (APE_CCL) 30
8.4.1 Evaluierung der Unteraufgabe (APE_CCL.1) 30
8.5 Sicherheitsproblemdefinition (APE_SPD) 37

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

8.5.1 Evaluierung der Unteraufgabe (APE_SPD.1) 37
8.6 Sicherheitszielsetzungen (APE_OBJ) 38
8.6.1 Evaluierung der Unteraufgabe (APE_OBJ.1) 38
8.6.2 Evaluierung der Unteraufgabe (APE_OBJ.2) 39
8.7 Erweiterte Komponentendefinition (APE_ECD) 41
8.7.1 Evaluierung der Unteraufgabe (APE_ECD.1) 41
8.8 Sicherheitsanforderungen (APE_REQ) 45
8.8.1 Evaluierung der Unteraufgabe (APE_REQ.1) 45
8.8.2 Evaluierung der Unteraufgabe (APE_REQ.2) 49

9 Klasse ASE: Evaluierung der Sicherheitsvorgabe 54
9.1 Einleitung 54
9.2 Anwendungshinweise 54
9.2.1 Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs 54
9.3 ST-Einleitung (ASE_INT) 54
9.3.1 Evaluierung der Unteraufgabe (ASE_INT.1) 54
9.4 Konformitätsansprüche (ASE_CCL) 57
9.4.1 Evaluierung der Unteraufgabe (ASE_CCL.1) 57
9.5 Sicherheitsproblemdefinition (ASE_SPD) 66
9.5.1 Evaluierung der Unteraufgabe (ASE_SPD.1) 66
9.6 Sicherheitszielsetzungen (ASE_OBJ) 67
9.6.1 Evaluierung der Unteraufgabe (ASE_OBJ.1) 67
9.6.2 Evaluierung der Unteraufgabe (ASE_OBJ.2) 68
9.7 Erweiterte Komponentendefinition (ASE_ECD) 70
9.7.1 Evaluierung der Unteraufgabe (ASE_ECD.1) 70
9.8 Sicherheitsanforderungen (ASE_REQ) 74
9.8.1 Evaluierung der Unteraufgabe (ASE_REQ.1) 74
9.8.2 Evaluierung der Unteraufgabe (ASE_REQ.2) 78
9.9 Zusammenfassende Spezifikation des TOEs (ASE_TSS) 83
9.9.1 Evaluierung der Unteraufgabe (ASE_TSS.1) 83
9.9.2 Evaluierung der Unteraufgabe (ASE_TSS.2) 83

10 Klasse ADV: Entwicklung 85
10.1 Einleitung 85
10.2 Anwendungshinweise 85
10.3 Sicherheitsarchitektur (ADV_ARC) 86
10.3.1 Evaluierung der Unteraufgabe (ADV_ARC.1) 86
10.4 Funktionsspezifikation (ADV_FSP) 91
10.4.1 Evaluierung der Unteraufgabe (ADV_FSP.1) 91
10.4.2 Evaluierung der Unteraufgabe (ADV_FSP.2) 94
10.4.3 Evaluierung der Unteraufgabe (ADV_FSP.3) 100
10.4.4 Evaluierung der Unteraufgabe (ADV_FSP.4) 105
10.4.5 Evaluierung der Unteraufgabe (ADV_FSP.5) 111
10.4.6 Evaluierung der Unteraufgabe (ADV_FSP.6) 118
10.5 Darstellung der Implementierung (ADV_IMP) 118
10.5.1 Evaluierung der Unteraufgabe (ADV_IMP.1) 118
10.5.2 Evaluierung der Unteraufgabe (ADV_IMP.2) 120
10.6 TSF-Interna (ADV_INT) 120
10.6.1 Evaluierung der Unteraufgabe (ADV_INT.1) 120
10.6.2 Evaluierung der Unteraufgabe (ADV_INT.2) 123
10.6.3 Evaluierung der Unteraufgabe (ADV_INT.3) 125
10.7 Modellierung der Sicherheitspolitik (ADV_SPM) 125
10.7.1 Evaluierung der Unteraufgabe (ADV_SPM.1) 125
10.8 TOE-Design (ADV_TDS) 125
10.8.1 Evaluierung der Unteraufgabe (ADV_TDS.1) 125
10.8.2 Evaluierung der Unteraufgabe (ADV_TDS.2) 129

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

10.8.3 Evaluierung der Unteraufgabe (ADV_TDS.3) ... 134
10.8.4 Evaluierung der Unteraufgabe (ADV_TDS.4) ... 144
10.8.5 Evaluierung der Unteraufgabe (ADV_TDS.5) ... 155
10.8.6 Evaluierung der Unteraufgabe (ADV_TDS.6) ... 155

11 Klasse AGD: Leitliniendokumente ... 155
11.1 Einleitung ... 155
11.2 Anwendungshinweise ... 155
11.3 Operative Leitlinien für Benutzer (AGD_OPE) ... 155
11.3.1 Evaluierung der Unteraufgabe (AGD_OPE.1) ... 155
11.4 Vorbereitende Verfahren (AGD_PRE) ... 158
11.4.1 Evaluierung der Unteraufgabe (AGD_PRE.1) ... 158

12 Klasse ALC: Unterstützung des Lebenszyklus ... 160
12.1 Einleitung ... 160
12.2 CM-Funktionen (ALC_CMC) ... 161
12.2.1 Evaluierung der Unteraufgabe (ALC_CMC.1) ... 161
12.2.2 Evaluierung der Unteraufgabe (ALC_CMC.2) ... 162
12.2.3 Evaluierung der Unteraufgabe (ALC_CMC.3) ... 164
12.2.4 Evaluierung der Unteraufgabe (ALC_CMC.4) ... 168
12.2.5 Evaluierung der Unteraufgabe (ALC_CMC.5) ... 174
12.3 CM-Umfang (ALC_CMS) ... 181
12.3.1 Evaluierung der Unteraufgabe (ALC_CMS.1) ... 181
12.3.2 Evaluierung der Unteraufgabe (ALC_CMS.2) ... 182
12.3.3 Evaluierung der Unteraufgabe (ALC_CMS.3) ... 183
12.3.4 Evaluierung der Unteraufgabe (ALC_CMS.4) ... 184
12.3.5 Evaluierung der Unteraufgabe (ALC_CMS.5) ... 185
12.4 Lieferung (ALC_DEL) ... 186
12.4.1 Evaluierung der Unteraufgabe (ALC_DEL.1) ... 186
12.5 Entwicklungssicherheit (ALC_DVS) ... 188
12.5.1 Evaluierung der Unteraufgabe (ALC_DVS.1) ... 188
12.5.2 Evaluierung der Unteraufgabe (ALC_DVS.2) ... 190
12.6 Mängelbeseitigung (ALC_FLR) ... 194
12.6.1 Evaluierung der Unteraufgabe (ALC_FLR.1) ... 194
12.6.2 Evaluierung der Unteraufgabe (ALC_FLR.2) ... 196
12.6.3 Evaluierung der Unteraufgabe (ALC_FLR.3) ... 200
12.7 Definition des Lebenszyklus (ALC_LCD) ... 206
12.7.1 Evaluierung der Unteraufgabe (ALC_LCD.1) ... 206
12.7.2 Evaluierung der Unteraufgabe (ALC_LCD.2) ... 207
12.8 Tools und Techniken (ALC_TAT) ... 209
12.8.1 Evaluierung der Unteraufgabe (ALC_TAT.1) ... 209
12.8.2 Evaluierung der Unteraufgabe (ALC_TAT.2) ... 211
12.8.3 Evaluierung der Unteraufgabe (ALC_TAT.3) ... 213

13 Klasse ATE: Prüfungen ... 216
13.1 Einleitung ... 216
13.2 Anwendungshinweise ... 216
13.2.1 Verständnis des erwarteten Verhaltens des TOEs ... 217
13.2.2 Prüfen gegenüber alternativen Ansätzen zur Überprüfung des erwarteten Verhaltens der Funktionalität ... 218
13.2.3 Überprüfung der Angemessenheit der Prüfungen ... 218
13.3 Abdeckung (ATE_COV) ... 219
13.3.1 Evaluierung der Unteraufgabe (ATE_COV.1) ... 219
13.3.2 Evaluierung der Unteraufgabe (ATE_COV.2) ... 219
13.3.3 Evaluierung der Unteraufgabe (ATE_COV.3) ... 221
13.4 Tiefe (ATE_DPT) ... 221
13.4.1 Evaluierung der Unteraufgabe (ATE_DPT.1) ... 221

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

13.4.2 Evaluierung der Unteraufgabe (ATE_DPT.2) ... 223
13.4.3 Evaluierung der Unteraufgabe (ATE_DPT.3) ... 226
13.4.4 Evaluierung der Unteraufgabe (ATE_DPT.4) ... 229
13.5 Funktionsprüfungen (ATE_FUN) ... 229
13.5.1 Evaluierung der Unteraufgabe (ATE_FUN.1) ... 229
13.5.2 Evaluierung der Unteraufgabe (ATE_FUN.2) ... 232
13.6 Unabhängiges Prüfen (ATE_IND) ... 232
13.6.1 Evaluierung der Unteraufgabe (ATE_IND.1) ... 232
13.6.2 Evaluierung der Unteraufgabe (ATE_IND.2) ... 237
13.6.3 Evaluierung der Unteraufgabe (ATE_IND.3) ... 242

14 Klasse AVA: Anfälligkeitsbewertung ... 242
14.1 Einleitung ... 242
14.2 Anfälligkeitsanalyse (AVA_VAN) ... 243
14.2.1 Evaluierung der Unteraufgabe (AVA_VAN.1) ... 243
14.2.2 Evaluierung der Unteraufgabe (AVA_VAN.2) ... 248
14.2.3 Evaluierung der Unteraufgabe (AVA_VAN.3) ... 255
14.2.4 Evaluierung der Unteraufgabe (AVA_VAN.4) ... 264
14.2.5 Evaluierung der Unteraufgabe (AVA_VAN.5) ... 272

15 Klasse ACO: Zusammensetzung ... 273
15.1 Einleitung ... 273
15.2 Anwendungshinweise ... 273
15.3 Begründung der Zusammensetzung (ACO_COR) ... 274
15.3.1 Evaluierung der Unteraufgabe (ACO_COR.1) ... 274
15.4 Entwicklungsnachweis (ACO_DEV) ... 281
15.4.1 Evaluierung der Unteraufgabe (ACO_DEV.1) ... 281
15.4.2 Evaluierung der Unteraufgabe (ACO_DEV.2) ... 282
15.4.3 Evaluierung der Unteraufgabe (ACO_DEV.3) ... 284
15.5 Verlässlichkeit der abhängigen Komponente (ACO_REL) ... 287
15.5.1 Evaluierung der Unteraufgabe (ACO_REL.1) ... 287
15.5.2 Evaluierung der Unteraufgabe (ACO_REL.2) ... 289
15.6 Prüfen des zusammengesetzten TOEs (ACO_CTT) ... 292
15.6.1 Evaluierung der Unteraufgabe (ACO_CTT.1) ... 292
15.6.2 Evaluierung der Unteraufgabe (ACO_CTT.2) ... 295
15.7 Anfälligkeitsanalyse der Zusammensetzung (ACO_VUL) ... 298
15.7.1 Evaluierung der Unteraufgabe (ACO_VUL.1) ... 298
15.7.2 Evaluierung der Unteraufgabe (ACO_VUL.2) ... 301
15.7.3 Evaluierung der Unteraufgabe (ACO_VUL.3) ... 305

Anhang A (informativ) Allgemeine Evaluierungsleitlinien ... 310
A.1 Zielsetzungen ... 310
A.2 Probenahme ... 310
A.3 Abhängigkeiten ... 312
A.3.1 Abhängigkeiten zwischen Aufgaben ... 312
A.3.2 Abhängigkeiten zwischen Unteraufgaben ... 312
A.3.3 Abhängigkeiten zwischen Aktionen ... 313
A.4 Standortbesichtigungen ... 313
A.4.1 Einleitung ... 313
A.4.2 Allgemeiner Ansatz ... 314
A.4.3 Orientierungshilfe für die Erstellung der Checkliste ... 314
A.4.4 Beispiel für eine Checkliste ... 316
A.5 Zuständigkeiten des Schemas ... 318

Anhang B (informativ) Anfälligkeitsbewertung (AVA) ... 320
B.1 Was ist eine Anfälligkeitsanalyse? ... 320
B.2 Erstellung einer Anfälligkeitsanalyse durch den Evaluator ... 321
B.2.1 Generische Leitlinien für Anfälligkeiten ... 321

Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

B.2.2 Identifizierung potentieller Anfälligkeiten 329
B.3 Wenn das Angriffspotential genutzt wird 332
B.3.1 Entwickler 332
B.3.2 Evaluator 332
B.4 Berechnung des Angriffspotentials 334
B.4.1 Anwendung des Angriffspotentials 334
B.4.2 Charakterisierung des Angriffspotentials 335
B.5 Beispielrechnung für direkten Angriff 341

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

Europäisches Vorwort

Der Text von ISO/IEC 18045:2008 wurde vom Technischen Komitee ISO/IEC JTC 1 „Information technology“ der Internationalen Organisation für Normung (ISO) und der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und als EN ISO/IEC 18045:2020 durch das Technische Komitee CEN/TC 13 „Cybersicherheit und Datenschutz“ übernommen, dessen Sekretariat von DIN gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis September 2020, und etwaige entgegenstehende nationale Normen müssen bis September 2020 zurückgezogen werden.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. CEN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Entsprechend der CEN-CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, die Republik Nordmazedonien, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Kroatien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Serbien, Slowakei, Slowenien, Spanien, Tschechische Republik, Türkei, Ungarn, Vereinigtes Königreich und Zypern.

Anerkennungsnotiz

Der Text von ISO/IEC 18045:2008 wurde von CEN als EN ISO/IEC 18045:2020 ohne irgendeine Abänderung genehmigt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

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. Auf dem Gebiet der Informationstechnologie haben ISO und IEC ein gemeinsames Technisches Komitee, ISO/IEC JTC 1 (JTC, en: Joint Technical Committee), eingerichtet.

Internationale Normen werden nach den Regeln der ISO/IEC-Direktiven, Teil 2 erarbeitet.

Die Hauptaufgabe des gemeinsamen Technischen Komitees (JTC, en: Joint Technical Committee) ist es, Internationale Normen zu erarbeiten. Die vom gemeinsamen Technischen Komitee verabschiedeten internationalen Norm-Entwürfe werden den nationalen Mitgliedern zur Abstimmung vorgelegt. Die Veröffentlichung als Internationale Norm erfordert Zustimmung von mindestens 75 % der abstimmenden nationalen Mitglieder.

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.

ISO/IEC 18045 wurde vom gemeinsamen Technischen Komitee ISO/IEC JTC 1, *Information technology*, Unterkomitee SC 27, *IT Security techniques,* erarbeitet. Der identische Text von ISO/IEC 18045 wird von den Common Criteria Project Sponsoring Organisations als *Gemeinsame Methodik für die Bewertung der IT-Sicherheit* (en: *Common Methodology for Information Technology Security Evaluation*) veröffentlicht. Die gemeinsame XML-Quelle für beide Publikationen befindet sich auf http://www.commoncriteriaportal.org/cc/.

Diese zweite Ausgabe ersetzt die erste Ausgabe (ISO/IEC 18045:2005), die technisch überarbeitet wurde.

Diese zweite korrigierte Version von ISO/IEC 18045:2008 enthält verschiedene redaktionelle Korrekturen in Bezug auf Folgendes:

— Konsistenz mit den korrigierten Versionen von ISO/IEC 15408-3:2008 und ISO/IEC 15408-1:2009;

— APE_CCL und ASE_CCL, APE_SPD und ASE_SPD, AGD_PRE, ALC_CMC, ALC_DVS, ADV_TDS, ASE_TSS, AVA_VAN und ADV_FSP.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

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, Version 3.1 (genannt CEM 3.1), gewähren sie der ISO/IEC hiermit eine nicht-exklusive Lizenz zur Nutzung von CEM 3.1 bei der Weiterentwicklung/Pflege der Internationalen Norm ISO/IEC 18045. Diese Regierungsorganisationen behalten jedoch das Recht, CEM 3.1 nach eigenem Ermessen zu nutzen, zu kopieren, zu verteilen, zu übersetzen oder zu modifizieren.

Australien/Neuseeland:	Das Defence Signals Directorate bzw. das Government Communications Security Bureau;
Kanada:	Communications Security Establishment;
Frankreich:	Direction Centrale 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;
Spanien:	Ministerio de Administraciones Públicas und Centro Criptológico Nacional;
Vereinigtes Königreich:	Communications-Electronic Security Group;
Vereinigte Staaten:	National Security Agency und National Institute of Standards and Technology.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

Einleitung

Die Zielgruppe für diese Internationale Norm sind in erster Linie Evaluatoren, die die ISO/IEC 15408 anwenden, und Zertifizierer, die die Evaluatorenaktionen bestätigen; Antragsteller der Evaluierung, Entwickler, PP-/ST-Autoren und andere an der IT-Sicherheit interessierte Parteien können eine sekundäre Zielgruppe sein.

Diese Internationale Norm erkennt an, dass hier nicht alle Fragen zur Evaluierung der IT-Sicherheit beantwortet werden und dass weitere Interpretationen notwendig sind. Einzelne Schemata legen fest, wie mit solchen Interpretationen umzugehen ist, auch wenn diese möglicherweise Gegenstand von Vereinbarungen über die gegenseitige Anerkennung sind. Eine Liste der methodenbezogenen Aufgaben, die im Rahmen der einzelnen Schemata durchgeführt werden können, findet sich in Anhang A.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

1 Anwendungsbereich

Diese Internationale Norm ist ein Begleitdokument zu den „Evaluierungskriterien für die IT-Sicherheit“, ISO/IEC 15408. Diese Internationale Norm legt die Aktionen fest, die ein Evaluator mindestens durchführen muss, um eine Evaluierung nach ISO/IEC 15408 unter Verwendung der in ISO/IEC 15408 definierten Kriterien und Evaluationsnachweise durchzuführen.

Diese Internationale Norm legt keine Evaluatorenaktionen für bestimmte Komponenten der ISO/IEC 15408 mit hoher Vertrauenswürdigkeit fest, für die es noch keine allgemein anerkannten Leitlinien gibt.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. 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 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

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

3.1
Aktion
Evaluatorenaktionselement aus ISO/IEC 15408-3

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

3.2
Aufgabe
Anwendung einer Vertrauenswürdigkeitsklasse aus ISO/IEC 15408-3

3.3
Prüfen
auf Grundlage eines einfachen Vergleichs eine **Entscheidung** treffen

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

3.4
Evaluationsbeitrag
Ressource, die der Evaluator oder die Evaluierungsinstanz vom Antragsteller oder Entwickler anfordert, um eine oder mehrere Evaluierungsaufgaben oder Evaluierungsüberwachungsaufgaben auszuführen

3.5
Evaluationsnachweis
konkreter **Evaluationsbeitrag**

3.6
Technischer Evaluierungsbericht
Bericht, in dem die vom Evaluator erstellte und bei einer Evaluierungsinstanz eingereichte **Gesamtentscheidung** einschließlich Begründung dokumentiert ist

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

3.7
Untersuchen
mittels Analyse und unter Nutzung von Evaluatoren-Fachwissen eine **Entscheidung** treffen

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

3.8
Interpretation
Klarstellung oder Erweiterung einer Anforderung aus ISO/IEC 15408, ISO/IEC 18045 oder aus dem **Schema**

3.9
Methodologie
System aus Vorgehensweisen, Verfahren und Prozessen, das für die IT-Sicherheitsevaluierung verwendet wird

3.10
Beobachtungsbericht
Bericht, der vom Evaluator verfasst wird, wenn dieser während der Evaluierung eine Klarstellung benötigt oder ein Problem identifiziert hat

3.11
Gesamtentscheidung
Urteil *„akzeptiert“ oder „abgelehnt“*, das ein Evaluator ausgehend vom Ergebnis einer Evaluierung fällt

3.12
Überwachungsentscheidung
Urteil, das von einer Evaluierungsinstanz gefällt wird und mit dem diese eine *Gesamtentscheidung* auf Grundlage der Ergebnisse von Evaluierungsüberwachungsaufgaben bestätigt oder ablehnt

3.13
Aufzeichnen
eine Beschreibung der Verfahren, Ereignisse, Beobachtungen, Erkenntnisse und Ergebnisse schriftlich festhalten, die so detailliert ist, dass die für die Evaluierung ausgeführten Arbeitsschritte damit zu einem späteren Zeitpunkt rekonstruiert werden können

3.14
Berichten
Evaluierungsergebnisse und dokumentierende Angaben und Unterlagen im **Technischen Evaluierungsbericht** oder einem **Beobachtungsbericht** zusammenstellen

3.15
Schema
Reihe von Regeln, die eine Evaluierungsinstanz zur Definition der Evaluierungsumgebung festlegt, einschließlich der für die Durchführung von IT-Sicherheitsevaluierungen erforderlichen Kriterien und **Methodologie**

3.16
Unteraufgabe
Anwendung einer Vertrauenswürdigkeitskomponente aus ISO/IEC 15408-3

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

3.17
Verfolgung
einfache direktionale Beziehung zwischen zwei Sätzen von Entitäten, die zeigt, welche Entitäten des ersten Satzes welchen Entitäten des zweiten Satzes entsprechen

3.18
Entscheidung
Urteil *„akzeptiert“, „abgelehnt“ oder „nicht bewertbar“*, das ein Evaluator hinsichtlich eines Evaluatorenaktionselements oder einer Vertrauenswürdigkeitskomponente oder -klasse fällt

ANMERKUNG Siehe auch **Gesamtentscheidung**.

3.19
Workunit
Ebene der kleinsten Einheiten bei der Durchführung der Evaluierung

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

4 Symbole und Abkürzungen

ETR **Technischer Evaluierungsbericht (en: evaluation technical report)**

OR Beobachtungsbericht (en: observation report)

5 Überblick

5.1 Gliederung dieser Internationalen Norm

Abschnitt 6 definiert die in dieser Internationalen Norm verwendeten Konventionen.

Abschnitt 7 beschreibt allgemeine Evaluierungsarbeitsaufgaben, mit denen keine Entscheidungen verbunden sind, da sie nicht auf die Evaluatorenaktionselemente nach ISO/IEC 15408 abgebildet werden.

Abschnitt 8 befasst sich mit der Arbeit, die zur Erzielung eines Evaluierungsergebnisses an einem PP erforderlich ist.

Abschnitt 9 bis Abschnitt 15 legen die Evaluierungsaufgaben fest, die von Vertrauenswürdigkeitsklassen organisiert werden.

Anhang A deckt die grundlegenden Evaluierungstechniken ab, die für den technischen Nachweis der Evaluierungsergebnisse verwendet werden.

Anhang B bietet eine Erläuterung der Kriterien der Anfälligkeitsanalyse und Beispiele für deren Anwendung.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

6 Typographische Konventionen

6.1 Terminologie

Im Gegensatz zur ISO/IEC 15408, bei der jedes Element die letzte Stelle seines Identifizierungssymbols für alle Komponenten innerhalb der Familie beibehält, kann diese Internationale Norm neue Workunits einführen, wenn ein Evaluatorenaktionselement der 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 den Anforderungen der ISO/IEC 15408 abgeleitet ist, wird als *Arbeitsaufgabe* oder *Teilarbeitsaufgabe* bezeichnet.

6.2 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 der ISO/IEC 15408 in einer Evaluierung. Der Verbgebrauch erfolgt in Übereinstimmung mit ISO-Definitionen für diese Verben. Das Hilfsverb *sollte* wird verwendet, wenn das beschriebene Verfahren stark bevorzugt wird. Alle anderen Hilfsverben, einschließlich *dürfen*, werden dort verwendet, wo das/die beschriebene(n) Verfahren erlaubt, aber weder empfohlen noch stark bevorzugt wird/werden; es handelt sich lediglich um eine Erläuterung.

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

6.3 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.

6.4 Beziehung zwischen den Strukturen von ISO/IEC 15408 und ISO/IEC 18045

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

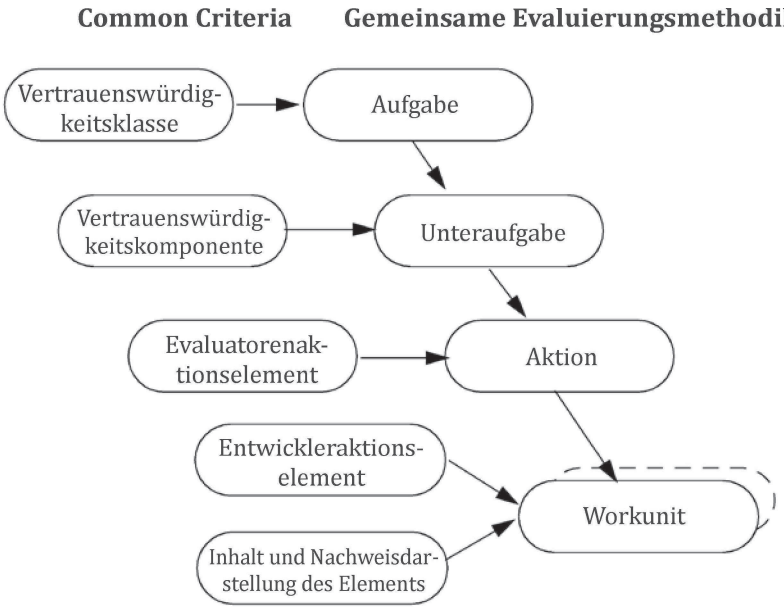

Bild 1 — Abbildung der Strukturen von ISO/IEC 15408 und ISO/IEC 18045

7 Evaluierungsprozess und damit verbundene Arbeitsaufgaben

7.1 Einleitung

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 oder TOE (einschließlich ST), folgt dem gleichen Prozess und hat vier Evaluierungsarbeitsaufgaben gemeinsam: die Eingabearbeitsaufgabe, die Ausgabearbeitsaufgabe, die Evaluierungsunteraufgaben und die Vorführung der technischen Kompetenz gegenüber der Arbeitsaufgabe der Evaluierungsinstanz.

Die Eingabearbeitsaufgabe 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 der ISO/IEC 15408 (Evaluierung eines PP oder eines TOE) gelten und für diese normativ sind.

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

Im Gegensatz zu den Evaluierungsunteraufgaben sind mit den Eingabe- und Ausgabearbeitsaufgaben keine Entscheidungen verbunden, da sie nicht auf die Evaluatorenaktionselemente der ISO/IEC 15408 abbilden; sie werden durchgeführt, um die Übereinstimmung mit den universellen Grundsätzen und die Einhaltung dieser Internationalen Norm sicherzustellen.

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 Evaluatorinstanz. Die detaillierten Kriterien zur Absolvierung dieser Arbeitsaufgabe liegen im Ermessen der Evaluierungsinstanz, wie in Anhang 0 angegeben.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

7.2 Überblick über den Evaluierungsprozess

7.2.1 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.

7.2.2 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.

7.2.3 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.

7.2.4 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

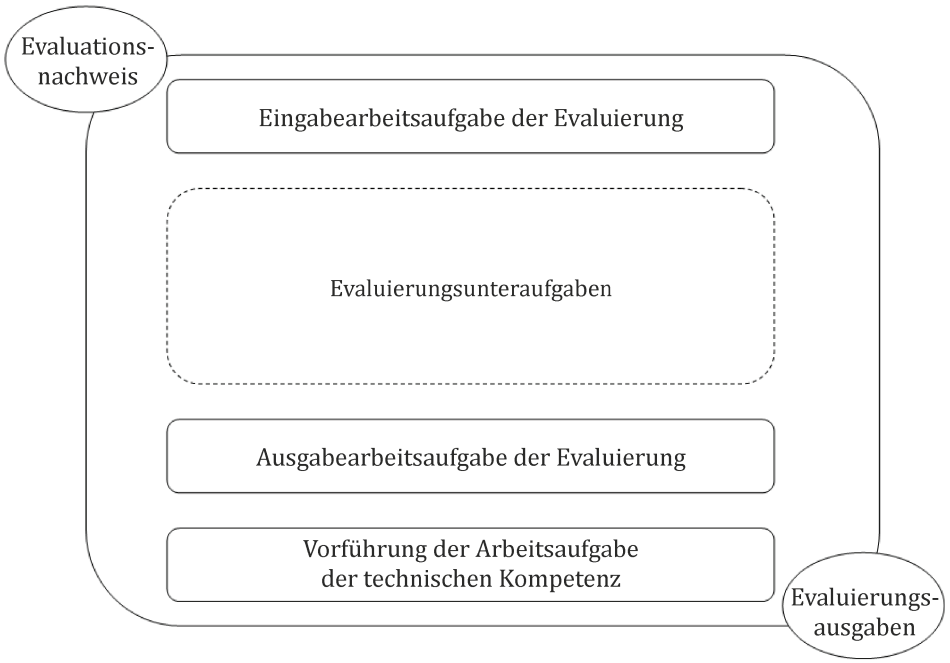

Bild 2 — Generisches Evaluierungsmodell

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.

7.2.5 Evaluatoren-Entscheidungen

Der Evaluator ordnet die Entscheidungen den Anforderungen der ISO/IEC 15408 und nicht denen dieser Internationalen Norm zu. Die kleinste Einheit der Struktur der ISO/IEC 15408, der eine Entscheidung zugeordnet wird, ist das Evaluatorenaktionselement (explizit oder implizit). Eine Entscheidung wird einem zutreffenden Evaluatorenaktionselement der ISO/IEC 15408 als Ergebnis der Durchführung der entsprechenden Aktion der Evaluierungsmethodik und der Workunits zugeordnet, aus denen sie besteht. Schließlich wird ein Evaluierungsergebnis zugeordnet, wie in ISO/IEC 15408-1, Abschnitt 9, Evaluierungsergebnisse, beschrieben.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

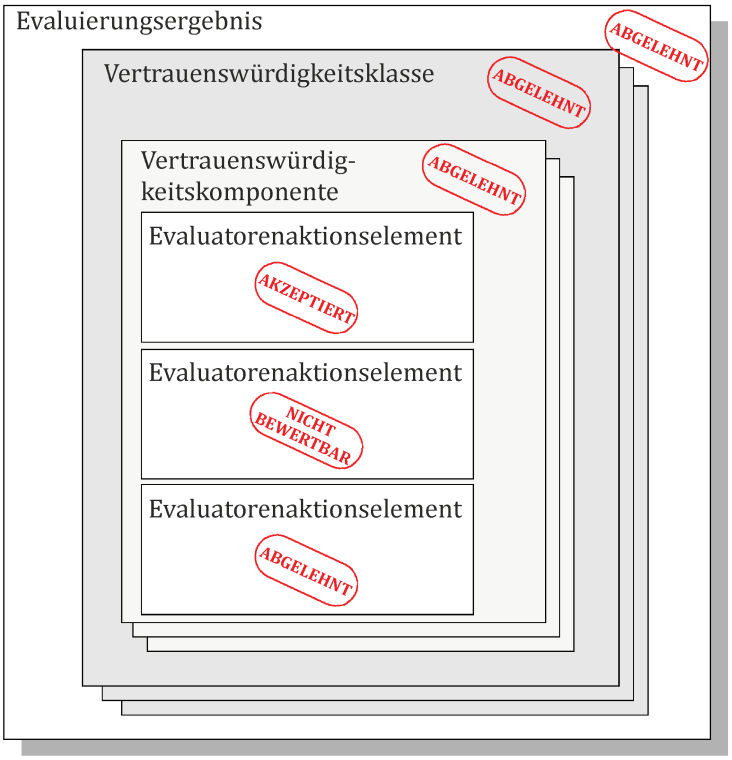

Bild 3 — Beispiel der Entscheidungszuordnungsregel

Diese Internationale Norm erkennt drei sich gegenseitig ausschließende Entscheidungszustände an:

a) Die Bedingungen für eine „*akzeptiert*"-Entscheidung sind definiert als die Vervollständigung des Evaluatorenaktionselements der ISO/IEC 15408 durch den Evaluator und die Feststellung, dass die Anforderungen an das/die zu evaluierende PP, 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 der ISO/IEC 15408 durch den Evaluator und die Feststellung, dass die Anforderungen an das/die zu evaluierende PP, 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*".

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

7.3 Eingabearbeitsaufgabe der Evaluierung

7.3.1 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.

7.3.2 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 TOEs 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 TOEs 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 TOEs-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 TOEs gleichzeitig mit seiner Entwicklung durchgeführt wird. Er kann jedoch auch während der Evaluierung eines bereits entwickelten TOEs 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 der ISO/IEC 15408 zu erfüllen).

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

7.3.3 Management der Teilarbeitsaufgabe der Evaluationsnachweise

7.3.3.1 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.

7.3.3.2 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.

7.3.3.3 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.

7.4 Evaluierungsunteraufgaben

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

7.5 Ausgabearbeitsaufgabe der Evaluierung

7.5.1 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. Diese Internationale Norm 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

Der Evaluator führt die beiden folgenden Teilarbeitsaufgaben durch, um die Anforderungen dieser Internationalen Norm an den Informationsgehalt von Berichten zu erfüllen:

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

b) ETR-Teilarbeitsaufgabe schreiben.

7.5.2 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.

7.5.3 Anwendungshinweise

In dieser Version dieser Internationalen Norm 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.

7.5.4 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).

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

7.5.5 ETR-Teilarbeitsaufgabe schreiben

7.5.5.1 Zielsetzungen

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

Diese Internationale Norm 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, der ISO/IEC 15408, dieser Internationalen Norm, 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 dieser Internationalen Norm.

7.5.5.2 ETR für eine PP-Evaluierung

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.

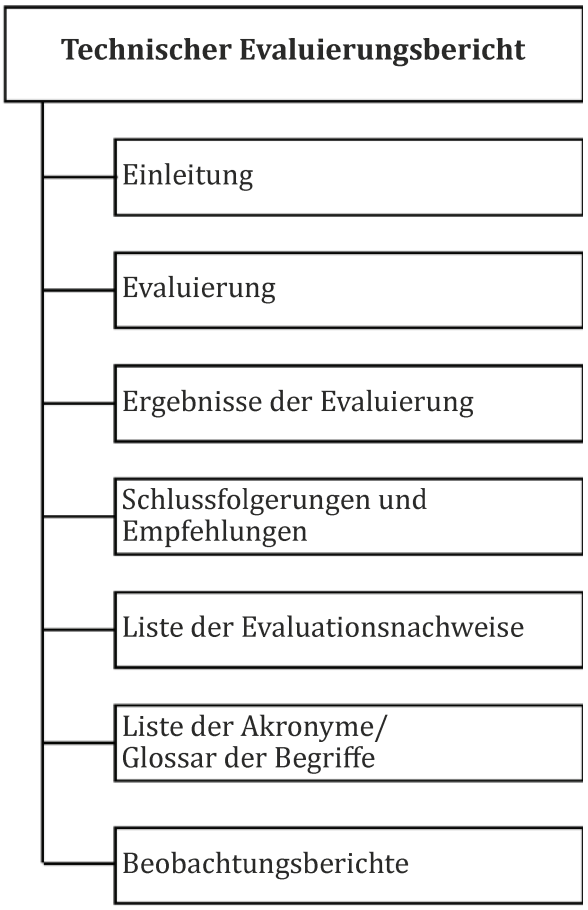

Bild 4 — ETR-Informationsgehalt für eine PP-Evaluierung

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

7.5.5.2.1 Einleitung

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.

7.5.5.2.2 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 usw. einbeziehen.

7.5.5.2.3 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 der ISO/IEC 15408, dieser Internationalen Norm, 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

7.5.5.2.4 Schlussfolgerungen und Empfehlungen

Der Evaluator ***muss*** die Schlussfolgerungen der Evaluierung, insbesondere die Gesamtentscheidung ***angeben***, wie in ISO/IEC 15408-1 Abschnitt 9, Evaluierungsergebnisse, festgelegt, und durch die Anwendung der in 7.2.5 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.

7.5.5.2.5 Liste der Evaluationsnachweise

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

— die Ausgabestelle (z. B. der Entwickler, der Antragsteller);

— den Titel;

— die eindeutige Verweisung (z. B. Ausgabedatum und Versionsnummer).

7.5.5.2.6 Liste der Akronyme/Glossar der Begriffe

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

Von ISO/IEC 15408 oder dieser Internationalen Norm bereits festgelegte Glossardefinitionen müssen im ETR nicht wiederholt werden.

7.5.5.2.7 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.

7.5.5.3 ETR für eine TOE-Evaluierung

In diesem Unterabschnitt wird der Mindestinhalt des ETR für eine TOE-Evaluierung beschrieben. Der Inhalt des ETR ist in Bild 5 dargestellt; dieses Bild kann als Leitfaden beim Aufbau der Struktur des ETR-Dokuments verwendet werden.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

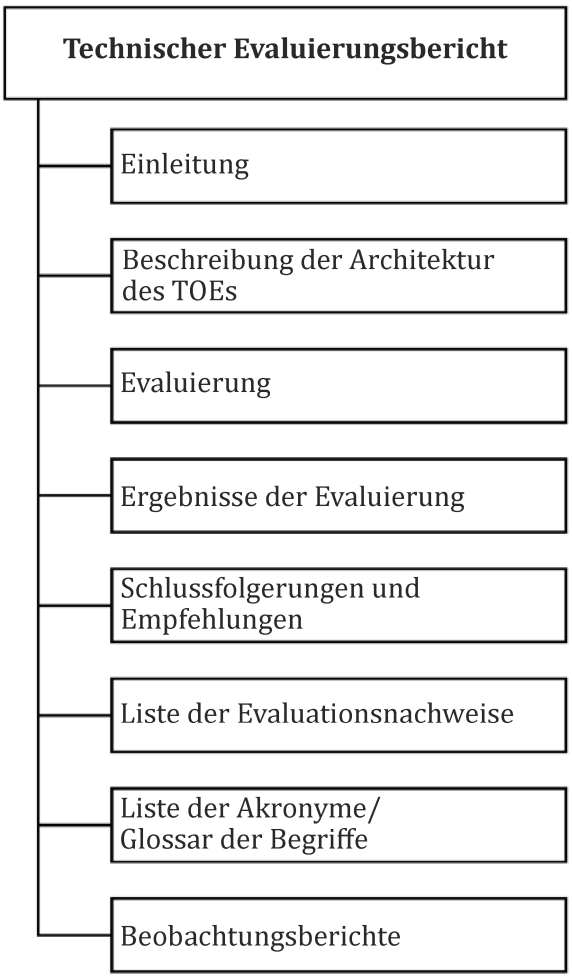

Bild 5 — ETR-Informationsgehalt für eine TOE-Evaluierung

7.5.5.3.1 Einleitung

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 PPs übereinstimmt, muss der ETR die Verweisung der entsprechenden PPs melden.

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

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

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

Die Identität des TOEs-Entwicklers wird benötigt, um die verantwortliche Partei für die Erstellung des TOEs 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.

7.5.5.3.2 Beschreibung der Architektur des TOEs

Der Evaluator ***muss,*** soweit zutreffend, eine allgemeine Beschreibung des TOEs 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.

7.5.5.3.3 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 TOEs oder der zur Durchführung der Prüfungen verwendeten Geräte verwendet werden.

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 usw. einbeziehen.

7.5.5.3.4 Ergebnisse der Evaluierung

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

— die Bezeichnung der in Betracht gezogenen Aufgabe;

— 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 der ISO/IEC 15408, dieser Internationalen Norm, 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.

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

7.5.5.3.5 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 Abschnitt 9, Evaluierungsergebnisse, die durch die Anwendung der in 7.2.5 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.

7.5.5.3.6 Liste der Evaluationsnachweise

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

— die Ausgabestelle (z. B. der Entwickler, der Antragsteller);

— den Titel;

— die eindeutige Verweisung (z. B. Ausgabedatum und Versionsnummer).

7.5.5.3.7 Liste der Akronyme/Glossar der Begriffe

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

Von ISO/IEC 15408 oder dieser Internationalen Norm bereits festgelegte Glossardefinitionen müssen im ETR nicht wiederholt werden.

7.5.5.3.8 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.

8 Klasse APE: Evaluierung des Schutzprofils

8.1 Einleitung

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, Klasse APE festgelegt.

Dieser Abschnitt sollte zusammen mit Anhang A, Anhang B und Anhang C, Leitlinien für Operationen, in ISO/IEC 15408-1 verwendet werden, da diese Anhänge die Begriffe hier verdeutlichen und viele Beispiele liefern.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

8.2 Anwendungshinweise

8.2.1 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.

8.3 PP-Einleitung (APE_INT)

8.3.1 Evaluierung der Unteraufgabe (APE_INT.1)

8.3.1.1 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.

8.3.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist

a) das PP.

8.3.1.3 Aktion APE_INT.1.1E

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

8.3.1.3.1 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 APE_INT.1.2C: *Die PP-Verweisung muss das PP eindeutig identifizieren.*

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

8.3.1.3.2 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 APE_INT.1.3C: *Der TOE-Überblick muss die Verwendung und wesentliche Sicherheitsmerkmale des TOEs zusammenfassen.*

8.3.1.3.3 Workunit APE_INT.1-3

Der Evaluator ***muss*** den TOE-Überblick ***untersuchen***, um festzustellen, dass er die Verwendung und die wichtigsten Sicherheitsmerkmale des TOEs 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 TOEs klar genug ist und ausreicht, um ihnen ein allgemeines Verständnis der beabsichtigten Verwendung und der wichtigsten Sicherheitsmerkmale des TOEs zu vermitteln.

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

8.3.1.3.4 Workunit APE_INT.1-4

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

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

8.3.1.3.5 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

8.4 Konformitätsansprüche (APE_CCL)

8.4.1 Evaluierung der Unteraufgabe (APE_CCL.1)

8.4.1.1 Zielsetzungen

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

8.4.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist

a) das PP,

b) das/die PP(s), mit dem/denen das PP Konformität beansprucht,

c) das/die Paket(e), mit dem/denen das PP Konformität beansprucht.

8.4.1.3 Aktion APE_CCL.1.1E

ISO/IEC 15408-3 APE_CCL.1.1C: *Der Konformitätsanspruch muss einen Konformitätsanspruch nach ISO/IEC 15408 enthalten, der die Version der ISO/IEC 15408 angibt, mit der das PP Konformität beansprucht.*

8.4.1.3.1 Workunit APE_CCL.1-1

Der Evaluator ***muss prüfen***, ob der Konformitätsanspruch einen Konformitätsanspruch nach ISO/IEC 15408 enthält, der die Version der ISO/IEC 15408 identifiziert, mit der das PP Konformität beansprucht.

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

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

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

8.4.1.3.3 Workunit APE_CCL.1-3

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

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

8.4.1.3.4 Workunit APE_CCL.1-4

Der Evaluator ***muss*** den Konformitätsanspruch nach ISO/IEC 15408 mit der 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.

8.4.1.3.5 Workunit APE_CCL.1-5

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

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

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

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

8.4.1.3.6 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.

8.4.1.3.7 Workunit APE_CCL.1-7

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

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

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

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

ISO/IEC 15408-3 APE_CCL.1.6C: *Der Konformitätsanspruch muss jede Konformität des PP mit einem Paket entweder als Paket-konform oder als Paket-ergänzt beschreiben.*

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

8.4.1.3.8 Workunit APE_CCL.1-8

Der Evaluator ***muss prüfen***, ob der Konformitätsanspruch für jedes identifizierte Paket entweder den Anspruch Paketname-konform oder Paketname-ergänzt angibt.

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

Wenn der Anspruch auf Paketkonformität Paketname-konform enthält, stellt der Evaluator Folgendes fest.

a) Handelt es sich bei dem Paket um ein Sicherheitspaket, so enthält das PP alle im Paket enthaltenen SARs, aber keine zusätzlichen SARs.

b) Handelt es sich bei dem Paket um ein Funktionspaket, so enthält das PP alle im Paket enthaltenen SFRs, aber keine zusätzlichen SFRs.

Wenn der Anspruch auf Paketkonformität Paketname-ergänzt enthält, stellt der Evaluator Folgendes fest.

a) Handelt es sich bei dem Paket um ein Sicherheitspaket, dann enthält 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.

b) Handelt es sich bei dem Paket um ein Funktionspaket, so enthält das PP alle im Paket enthaltenen SFRs und mindestens eine zusätzliche SFR oder mindestens eine SFR, die hierarchisch zu einer SFR im Paket angeordnet ist.

ISO/IEC 15408-3 APE_CCL.1.7C: *Die Begründung für den Konformitätsanspruch muss nachweisen, dass der TOE-Typ mit dem TOE-Typ in den PPs konsistent ist, für die Konformität beansprucht wird.*

8.4.1.3.9 Workunit APE_CCL.1-9

Der Evaluator ***muss*** die Begründung für den Konformitätsanspruch ***untersuchen***, um festzustellen, dass der TOE-Typ des TOEs gegenüber allen TOE-Typen der PPs 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 PPs beansprucht: ein PP für die integrierte Schaltung, ein PP für das Betriebssystem einer Chipkarte und zwei PPs für zwei Anwendungen auf der Chipkarte.

ISO/IEC 15408-3 APE_CCL.1.8C: *Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zur Sicherheitsproblemdefinition mit der Aussage zur Sicherheitsproblemdefinition in den PPs konsistent ist, für die Konformität beansprucht wird.*

8.4.1.3.10 Workunit APE_CCL.1-10

Der Evaluator ***muss*** die Begründung für den Konformitätsanspruch ***untersuchen***, um festzustellen, dass sie die Konsistenz der Aussage der Sicherheitsproblemdefinition, wie sie in der Konformitätserklärung des PP festgelegt ist, gegenüber den Aussagen der Sicherheitsproblemdefinition in den PPs nachweist, mit denen Konformität beansprucht wird.

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

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

Wenn das PP, mit dem Konformität beansprucht wird, keine Aussage der Sicherheitsproblemdefinition enthält, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

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 den 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.

Bei der Untersuchung eines PP, bei der Annahmen aus einem anderen PP, mit dem Konformität beansprucht wird, weggelassen oder neue Annahmen hinzugefügt werden, muss der Evaluator genau ermitteln, ob die oben genannten Bedingungen erfüllt sind. Die folgende Erörterung liefert die Motivation und Beispiele für diese Fälle.

— 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 TOEs 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

— 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),

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

— 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 APE_CCL.1.9C: *Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zu den Sicherheitszielsetzungen mit der Aussage der Sicherheitszielsetzungen in den PPs konsistent ist, für die Konformität beansprucht wird.*

8.4.1.3.11 Workunit APE_CCL.1-11

Der Evaluator ***muss*** die Begründung für den Konformitätsanspruch ***untersuchen***, um festzustellen, dass die Aussage der Sicherheitszielsetzungen, wie sie in der Konformitätserklärung des PP festgelegt ist, gegenüber der Aussage der Sicherheitszielsetzungen in den PPs konsistent ist.

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

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

— 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,

— 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,

— 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,

— 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.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

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

— 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,

— 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),

— 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 APE_CCL.1.10C: *Die Begründung für den Konformitätsanspruch muss nachweisen, dass die Aussage zu den Sicherheitsanforderungen mit der Aussage zu den Sicherheitsanforderungen in den PPs konsistent ist, für die Konformität beansprucht wird.*

8.4.1.3.12 Workunit APE_CCL.1-12

Der Evaluator ***muss*** das PP ***untersuchen***, um festzustellen, ob es, wie in der Konformitätserklärung des PP definiert, gegenüber allen Sicherheitsanforderungen in den PPs, mit denen Konformität beansprucht wird, konsistent ist.

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

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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

— 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 APE_CCL.1.11C: *Die Konformitätserklärung muss die geforderte Konformität aller PPs/STs mit dem PP als strikte PP-Konformität oder nachweisliche PP-Konformität beschreiben.*

8.4.1.3.13 Workunit APE_CCL.1-13

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

8.5 Sicherheitsproblemdefinition (APE_SPD)

8.5.1 Evaluierung der Unteraufgabe (APE_SPD.1)

8.5.1.1 Zielsetzungen

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

8.5.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist

a) das PP.

8.5.1.3 Aktion APE_SPD.1.1E

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

8.5.1.3.1 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.

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

8.5.1.3.2 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.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

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 APE_SPD.1.3C: *Die Sicherheitsproblemdefinition muss die OSPs beschreiben.*

8.5.1.3.3 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 Grundsatzerklärungen ist notwendig, um die Rückverfolgung der Sicherheitszielsetzungen zu ermöglichen.

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

8.5.1.3.4 Workunit APE_SPD.1-4

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

8.6 Sicherheitszielsetzungen (APE_OBJ)

8.6.1 Evaluierung der Unteraufgabe (APE_OBJ.1)

8.6.1.1 Zielsetzungen

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

8.6.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist

a) das PP.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

8.6.1.3 Aktion APE_OBJ.1.1E

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

8.6.1.3.1 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.

8.6.2 Evaluierung der Unteraufgabe (APE_OBJ.2)

8.6.2.1 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.

8.6.2.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist

a) das PP.

8.6.2.3 Aktion APE_OBJ.2.1E

ISO/IEC 15408-3 APE_OBJ.2.1C: *Die Aussage zu Sicherheitszielsetzungen muss die Sicherheitszielsetzungen für den TOE und die Sicherheitszielsetzungen für die Betriebsumgebung beschreiben.*

8.6.2.3.1 Workunit APE_OBJ.2-1

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

Der Evaluator prüft, ob beide Kategorien von Sicherheitszielsetzungen klar identifiziert und von der anderen Kategorie getrennt sind.

ISO/IEC 15408-3 APE_OBJ.2.2C: *Die Begründung für die Sicherheitszielsetzungen muss jede Sicherheitszielsetzung für den TOE zurückführen zu den Bedrohungen, die durch diese Sicherheitszielsetzung abgewehrt werden, und zu den OSPs, die durch diese Sicherheitszielsetzung durchgesetzt werden.*

8.6.2.3.2 Workunit APE_OBJ.2-2

Der Evaluator ***muss prüfen***, ob die Begründung der Sicherheitszielsetzungen alle Sicherheitszielsetzungen für den TOE auf Bedrohungen zurückführt, denen die Zielsetzungen und/oder die durch die Zielsetzungen durchgesetzten OSPs entgegenwirken.

Jede Sicherheitszielsetzung für den TOE kann auf Bedrohungen oder OSPs bzw. auf eine Kombination von Bedrohungen und OSPs zurückführen, sie muss aber auf mindestens eine Bedrohung oder eine OSP zurückführen.

Eine fehlende Nachvollziehbarkeit bedeutet, dass entweder die Begründung der Sicherheitszielsetzungen unvollständig ist, dass die Sicherheitsproblemdefinition unvollständig ist oder dass die Sicherheitszielsetzung für den TOE keinen sinnvollen Zweck hat.

ISO/IEC 15408-3 APE_OBJ.2.3C: *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.*

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

8.6.2.3.3 Workunit APE_OBJ.2-3

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 Nachvollziehbarkeit 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.

ISO/IEC 15408-3 APE_OBJ.2.4C: *Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen alle Bedrohungen abwehren.*

8.6.2.3.4 Workunit APE_OBJ.2-4

Der Evaluator ***muss*** die Begründung der Sicherheitszielsetzungen ***untersuchen***, um festzustellen, ob sie für jede Bedrohung rechtfertigt, dass die Sicherheitszielsetzungen zur Abwehr dieser Bedrohung geeignet sind.

Wenn keine Sicherheitszielsetzungen auf die Bedrohung zurückgeführt werden können, wird die Evaluatorenaktion, die sich auf diese Workunit bezieht, mit einer „*abgelehnt*"-Entscheidung belegt.

Der Evaluator stellt fest, dass die Begründung für eine Bedrohung zeigt, ob die Bedrohung beseitigt, vermindert oder abgeschwächt wird.

Der Evaluator stellt fest, dass die Begründung für eine Bedrohung zeigt, dass die Sicherheitszielsetzungen ausreichend sind: Wenn alle Sicherheitszielsetzungen, die auf die Bedrohung zurückführen, erreicht werden, ist die Bedrohung beseitigt, ausreichend vermindert oder die Auswirkungen der Bedrohung werden ausreichend abgeschwächt.

Es ist zu beachten, dass die Rückverfolgungen von den Sicherheitszielsetzungen bis hin zu den Bedrohungen, die in der Begründung der Sicherheitszielsetzungen aufgeführt sind, Teil einer Begründung sein können, aber keine Begründung für sich selbst darstellen. Selbst für den Fall, dass eine Sicherheitszielsetzung lediglich eine Aussage ist, die die Absicht widerspiegelt, die Verwirklichung einer bestimmten Bedrohung zu verhindern, ist eine Begründung erforderlich, die jedoch so minimal sein kann wie „Sicherheitszielsetzung X wirkt der Bedrohung Y direkt entgegen".

Der Evaluator stellt auch fest, dass jede Sicherheitszielsetzung, die auf eine Bedrohung zurückführt, notwendig ist: Wenn die Sicherheitszielsetzung erreicht ist, trägt sie tatsächlich zur Beseitigung, Verminderung oder Abschwächung dieser Bedrohung bei.

ISO/IEC 15408-3 APE_OBJ.2.5C: *Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen alle OSPs durchsetzen.*

8.6.2.3.5 Workunit APE_OBJ.2-5

Der Evaluator ***muss*** die Begründung der Sicherheitszielsetzungen ***untersuchen***, um festzustellen, ob sie für jede OSP rechtfertigt, dass die Sicherheitszielsetzungen geeignet sind, diese OSP durchzusetzen.

Wenn keine Sicherheitszielsetzungen auf die OSP zurückgeführt werden können, wird die Evaluatorenaktion, die sich auf diese Workunit bezieht, mit einer „*abgelehnt*"-Entscheidung belegt.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

Der Evaluator stellt fest, dass die Begründung für eine OSP zeigt, dass die Sicherheitszielsetzungen ausreichend sind: Wenn alle Sicherheitszielsetzungen, die auf die OSP zurückführen, erreicht werden, wird die OSP durchgesetzt.

Der Evaluator stellt auch fest, dass jede Sicherheitszielsetzung, die auf eine OSP zurückführt, notwendig ist: Wenn die Sicherheitszielsetzung erreicht ist, trägt sie tatsächlich zur Durchsetzung der OSP bei.

Es ist zu beachten, dass die Rückverfolgungen von den Sicherheitszielsetzungen bis hin zu den OSPs, die in der Begründung der Sicherheitszielsetzungen aufgeführt sind, Teil einer Begründung sein können, aber keine Begründung für sich selbst darstellen. Für den Fall, dass eine Sicherheitszielsetzung lediglich eine Aussage ist, die die Absicht widerspiegelt, eine bestimmte OSP durchzusetzen, ist eine Begründung erforderlich, die jedoch so minimal sein kann wie „Sicherheitszielsetzung X setzt OSP Y direkt durch“.

ISO/IEC 15408-3 APE_OBJ.2.6C: *Die Begründung für die Sicherheitszielsetzungen muss nachweisen, dass die Sicherheitszielsetzungen für die Betriebsumgebung alle Annahmen einhalten.*

8.6.2.3.6 Workunit APE_OBJ.2-6

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 TOEs 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 TOEs 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 Rückverfolgungen von den Sicherheitszielsetzungen für die Betriebsumgebung bis hin zu den Annahmen, die in der Begründung der Sicherheitszielsetzungen aufgeführt sind, Teil einer Begründung sein können, aber keine Begründung für sich selbst darstellen. Selbst für den Fall, dass eine Sicherheitszielsetzung der Betriebsumgebung lediglich die Neuformulierung einer Annahme ist, ist eine Begründung erforderlich, die jedoch so minimal sein kann wie „Sicherheitszielsetzung X hält die Annahme Y direkt aufrecht“.

8.7 Erweiterte Komponentendefinition (APE_ECD)

8.7.1 Evaluierung der Unteraufgabe (APE_ECD.1)

8.7.1.1 Zielsetzungen

Die Zielsetzung dieser Unteraufgabe ist es, festzustellen, ob erweiterte Komponenten klar und eindeutig definiert wurden und ob sie notwendig sind, d. h. sie können unter Verwendung bestehender Komponenten der ISO/IEC 15408-2 oder ISO/IEC 15408-3 nicht klar ausgedrückt werden.

8.7.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist

a) das PP.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

8.7.1.3 Aktion APE_ECD.1.1E

ISO/IEC 15408-3 APE_ECD.1.1C: *Die Aussage zu den Sicherheitsanforderungen muss alle erweiterten Sicherheitsanforderungen identifizieren.*

8.7.1.3.1 Workunit APE_ECD.1-1

Der Evaluator ***muss prüfen***, ob alle Sicherheitsanforderungen in der Aussage der Sicherheitsanforderungen, die nicht als erweiterte Anforderungen gekennzeichnet sind, in der ISO/IEC 15408-2 oder in der ISO/IEC 15408-3 enthalten sind.

ISO/IEC 15408-3 APE_ECD.1.2C: *Die erweiterte Komponentendefinition muss für jede erweiterte Sicherheitsanforderung eine erweiterte Komponente definieren.*

8.7.1.3.2 Workunit APE_ECD.1-2

Der Evaluator ***muss prüfen***, ob die erweiterte Komponentendefinition für jede erweiterte Sicherheitsanforderung eine erweiterte Komponente definiert.

Enthält das PP keine erweiterten Sicherheitsanforderungen, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Eine einzelne erweiterte Komponente kann verwendet werden, um mehrfache Iterationen einer erweiterten Sicherheitsanforderung zu definieren, es ist nicht notwendig, diese Definition für jede Iteration zu wiederholen.

ISO/IEC 15408-3 APE_ECD.1.3C: *Die erweiterte Komponentendefinition muss beschreiben, wie jede erweiterte Komponente mit den bestehenden Komponenten, Familien und Klassen der ISO/IEC 15408 in Beziehung steht.*

8.7.1.3.3 Workunit APE_ECD.1-3

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass sie beschreibt, wie jede erweiterte Komponente in die vorhandenen Komponenten, Familien und Klassen der ISO/IEC 15408 passt.

Enthält das PP keine erweiterten Sicherheitsanforderungen, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass jede erweiterte Komponente entweder

a) ein Mitglied einer bestehenden Familie der ISO/IEC 15408-2 oder ISO/IEC 15408-3 ist, oder

b) ein Mitglied einer neuen, im PP definierten Familie.

Wenn die erweiterte Komponente Mitglied einer bestehenden Familie der ISO/IEC 15408-2 oder ISO/IEC 15408-3 ist, stellt der Evaluator fest, dass die erweiterte Komponentendefinition angemessen beschreibt, warum die erweiterte Komponente ein Mitglied dieser Familie sein sollte und wie sie mit anderen Komponenten dieser Familie zusammenhängt.

Wenn die erweiterte Komponente ein Mitglied einer neuen, im PP definierten Familie ist, bestätigt der Evaluator, dass die erweiterte Komponente nicht für eine bestehende Familie geeignet ist.

Wenn das PP neue Familien definiert, stellt der Evaluator fest, dass jede neue Familie entweder

a) ein Mitglied einer bestehenden Klasse der ISO/IEC 15408-2 oder ISO/IEC 15408-3 ist, oder

b) ein Mitglied einer neuen, im PP definierten Klasse.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

Wenn die Familie ein Mitglied einer bestehenden Klasse der ISO/IEC 15408-2 oder ISO/IEC 15408-3 ist, stellt der Evaluator fest, dass die erweiterte Komponentendefinition angemessen beschreibt, warum die Familie ein Mitglied jener Klasse sein sollte und wie sie mit anderen Familien jener Klasse zusammenhängt.

Wenn die Familie ein Mitglied einer neuen, im PP definierten Klasse ist, bestätigt der Evaluator, dass die Familie für eine bestehende Klasse nicht geeignet ist.

8.7.1.3.4 Workunit APE_ECD.1-4

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass jede Definition einer erweiterten Komponente alle anwendbaren Abhängigkeiten dieser Komponente identifiziert.

Enthält das PP keine erweiterten Sicherheitsanforderungen, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator bestätigt, dass der PP-Autor keine zutreffenden Abhängigkeiten übersehen hat.

ISO/IEC 15408-3 APE_ECD.1.4C: *Die erweiterte Komponentendefinition muss die bestehendenen Komponenten, Familien, Klassen und die Methodik der ISO/IEC 15408 als ein Modell der Darstellung verwenden.*

8.7.1.3.5 Workunit APE_ECD.1-5

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass jede erweiterte Funktionskomponente die vorhandenen Komponenten der ISO/IEC 15408-2 als Modell für die Darstellung verwendet.

Enthält das PP keine erweiterten SFRs, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass jede erweiterte Funktionskomponente konsistent ist gegenüber ISO/IEC 15408-2, 6.1.3, Komponentenstruktur.

Wenn die erweiterte Funktionskomponente Operationen verwendet, stellt der Evaluator fest, dass die erweiterte Funktionskomponente konsistent ist gegenüber ISO/IEC 15408-1, 7.1, Operationen.

Wenn die erweiterte Funktionskomponente hierarchisch zu einer bestehenden Funktionskomponente ist, stellt der Evaluator fest, dass die erweiterte Funktionskomponente konsistent ist gegenüber ISO/IEC 15408-2, 6.2.1, Hervorheben von Komponentenänderungen.

8.7.1.3.6 Workunit APE_ECD.1-6

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass jede Definition einer neuen Funktionsfamilie die bestehenden Funktionsfamilien der ISO/IEC 15408 als Modell für die Darstellung verwendet.

Wenn das PP keine neuen Funktionsfamilien definiert, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass alle neuen Funktionsfamilien konsistent definiert werden gegenüber ISO/IEC 15408-2, 6.1.2, Familienstruktur.

8.7.1.3.7 Workunit APE_ECD.1-7

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass jede Definition einer neuen Funktionsklasse die bestehenden Funktionsklassen der ISO/IEC 15408 als Modell für die Darstellung verwendet.

Wenn das PP keine neuen Funktionsklassen definiert, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass alle neuen Funktionsklassen konsistent definiert werden gegenüber ISO/IEC 15408-2, 6.1.1, Klassenstruktur.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

8.7.1.3.8 Workunit APE_ECD.1-8

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass jede Definition einer erweiterten Vertrauenswürdigkeitskomponente die vorhandenen Komponenten der ISO/IEC 15408-3 als Modell für die Darstellung verwendet.

Enthält das PP keine erweiterten SARs, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass jede erweiterte Vertrauenswürdigkeitskomponente konsistent ist gegenüber ISO/IEC 15408-3, 6.1.3, Struktur der Vertrauenswürdigkeitskomponenten.

Wenn die erweiterte Vertrauenswürdigkeitskomponente Operationen verwendet, stellt der Evaluator fest, dass die erweiterte Vertrauenswürdigkeitskomponente konsistent ist gegenüber ISO/IEC 15408-1, 7.1, Operationen.

Wenn die erweiterte Vertrauenswürdigkeitskomponente hierarchisch zu einer bestehenden Vertrauenswürdigkeitskomponente ist, stellt der Evaluator fest, dass die erweiterte Vertrauenswürdigkeitskomponente konsistent ist gegenüber ISO/IEC 15408-3, 6.1.3, Struktur der Vertrauenswürdigkeitskomponenten.

8.7.1.3.9 Workunit APE_ECD.1-9

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, ob für jede definierte erweiterte Vertrauenswürdigkeitskomponente eine anwendbare Methodik bereitgestellt wurde.

Enthält das PP keine erweiterten SARs, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass für jedes Evaluatorenaktionselement jeder erweiterten SAR eine oder mehrere Workunits vorgesehen sind und dass die erfolgreiche Durchführung aller Workunits für ein bestimmtes Evaluatorenaktionselement nachweisen wird, dass das Element erreicht wurde.

8.7.1.3.10 Workunit APE_ECD.1-10

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass jede Definition einer neuen Vertrauenswürdigkeitsfamilie die bestehenden Vertrauenswürdigkeitsfamilien der ISO/IEC 15408 als Modell für die Darstellung verwendet.

Wenn das PP keine neuen Vertrauenswürdigkeitsfamilien definiert, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass alle neuen Vertrauenswürdigkeitsfamilien konsistent definiert werden gegenüber ISO/IEC 15408-3, 6.1.2, Struktur der Vertrauenswürdigkeitsfamilien.

8.7.1.3.11 Workunit APE_ECD.1-11

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass jede Definition einer neuen Vertrauenswürdigkeitsklasse die bestehenden Vertrauenswürdigkeitsklassen der ISO/IEC 15408 als Modell für die Darstellung verwendet.

Wenn das PP keine neuen Vertrauenswürdigkeitsklassen definiert, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass alle neuen Vertrauenswürdigkeitsklassen konsistent definiert werden gegenüber ISO/IEC 15408-3, 6.1.1, Struktur der Vertrauenswürdigkeitsklassen.

ISO/IEC 15408-3 APE_ECD.1.5C: *Die erweiterten Komponenten müssen aus messbaren und objektiven Elementen bestehen, sodass die Konformität oder Nichtkonformität mit diesen Elementen nachgewiesen werden kann.*

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

8.7.1.3.12 Workunit APE_ECD.1-12

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass jedes Element in jeder erweiterten Komponente messbar ist und objektive Evaluierungsanforderungen angibt, so dass Konformität oder Nichtkonformität nachgewiesen werden kann.

Enthält das PP keine erweiterten Sicherheitsanforderungen, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator stellt fest, dass die Elemente der erweiterten Funktionskomponenten so angegeben werden, dass sie prüfbar und durch die entsprechenden TSF-Darstellungen rückverfolgbar sind.

Der Evaluator stellt auch fest, dass Elemente der erweiterten Vertrauenswürdigkeitskomponenten die Notwendigkeit einer subjektiven Beurteilung durch den Evaluator vermeiden.

Der Evaluator wird daran erinnert, dass alle Evaluierungskriterien zwar messbar und objektiv sind, dass es aber anerkanntermaßen kein formales Verfahren zum Nachweis solcher Eigenschaften gibt. Daher sind die vorhandenen Funktions- und Vertrauenswürdigkeitskomponenten der ISO/IEC 15408 als Modell für die Bestimmung der Konformität mit dieser Anforderung zu verwenden.

8.7.1.4 Aktion APE_ECD.1.2E

8.7.1.4.1 Workunit APE_ECD.1-13

Der Evaluator ***muss*** die erweiterte Komponentendefinition ***untersuchen***, um festzustellen, dass jede erweiterte Komponente nicht eindeutig durch vorhandene Komponenten ausgedrückt werden kann.

Enthält das PP keine erweiterten Sicherheitsanforderungen, ist diese Workunit nicht anwendbar und gilt daher als erfüllt.

Der Evaluator sollte bei dieser Bestimmung Komponenten aus ISO/IEC 15408-2 und ISO/IEC 15408-3, andere erweiterte Komponenten, die im PP definiert wurden, Kombinationen dieser Komponenten und mögliche Operationen an diesen Komponenten berücksichtigen.

Der Evaluator wird daran erinnert, dass die Rolle dieser Workunit darin besteht, eine unnötige Duplizierung von Komponenten zu vermeiden, d. h. von Komponenten, die durch die Verwendung anderer Komponenten klar ausgedrückt werden können. Der Evaluator sollte keine erschöpfende Suche nach allen möglichen Kombinationen von Komponenten einschließlich Operationen durchführen, um zu versuchen, einen Weg zu finden, die erweiterte Komponente durch Verwendung vorhandener Komponenten auszudrücken.

8.8 Sicherheitsanforderungen (APE_REQ)

8.8.1 Evaluierung der Unteraufgabe (APE_REQ.1)

8.8.1.1 Zielsetzungen

Die Zielsetzung dieser Unteraufgabe besteht darin, festzustellen, ob die SFRs und SARs klar, eindeutig und genau definiert sind und ob sie in sich konsistent sind.

8.8.1.2 Eingaben

Der Evaluationsnachweis für diese Unteraufgabe ist

a) das PP.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

8.8.1.3 Aktion APE_REQ.1.1E

ISO/IEC 15408-3 APE_REQ.1.1C: *Die Aussage zu den Sicherheitsanforderungen muss die SFRs und die SARs beschreiben.*

8.8.1.3.1 Workunit APE_REQ.1-1

Der Evaluator ***muss prüfen***, ob die Aussage der Sicherheitsanforderungen die SFRs beschreibt.

Der Evaluator stellt fest, dass jede SFR auf eine der folgenden Arten identifiziert wird:

a) durch Verweisung auf eine einzelne Komponente in ISO/IEC 15408-2;

b) durch Verweisung auf eine erweiterte Komponente in der erweiterten Komponentendefinition des PP;

c) durch Verweisung auf ein PP, mit dem das PP beansprucht, konform zu sein;

d) durch Verweisung auf ein Sicherheitsanforderungspaket, mit dem das PP beansprucht, konform zu sein;

e) durch Vervielfältigung im PP.

Es ist nicht erforderlich, für alle SFRs das gleiche Identifizierungsmittel zu verwenden.

8.8.1.3.2 Workunit APE_REQ.1-2

Der Evaluator ***muss prüfen***, ob die Aussage der Sicherheitsanforderungen die SARs beschreibt.

Der Evaluator stellt fest, dass jede SAR auf eine der folgenden Arten identifiziert wird:

a) durch Verweisung auf eine einzelne Komponente in ISO/IEC 15408-3;

b) durch Verweisung auf eine erweiterte Komponente in der erweiterten Komponentendefinition des PP;

c) durch Verweisung auf ein PP, mit dem das PP beansprucht, konform zu sein;

d) durch Verweisung auf ein Sicherheitsanforderungspaket, mit dem das PP beansprucht, konform zu sein;

e) durch Vervielfältigung im PP.

Es ist nicht erforderlich, für alle SARs das gleiche Identifizierungsmittel zu verwenden.

ISO/IEC 15408-3 APE_REQ.1.2C: *Alle Subjekte, Objekte, Operationen, Sicherheitsattribute, externen Entitäten und sonstigen in den SFRs und SARs verwendeten Begriffe müssen definiert sein.*

8.8.1.3.3 Workunit APE_REQ.1-3

Der Evaluator ***muss*** das PP ***untersuchen***, um festzustellen, ob alle Subjekte, Objekte, Operationen, Sicherheitsattribute, externen Entitäten und sonstigen Begriffe, die in den SFRs und den SARs verwendet werden, definiert sind.

Der Evaluator stellt fest, dass das PP Folgendes definiert:

— alle (Arten von) Subjekte(n) und Objekte(n), die in den SFRs verwendet werden;

— alle (Arten von) Sicherheitsattribute(n) von Subjekten, Benutzern, Objekten, Informationen, Sitzungen und/oder Ressourcen, mögliche Werte, die diese Attribute annehmen können, und alle Beziehungen zwischen diesen Werten (z. B. ist streng_geheim „höher“ als geheim);

AVA Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02

— alle (Arten von) Operationen, die in den SFRs verwendet werden, einschließlich der Auswirkungen dieser Operationen;

— alle (Arten von) externen Entitäten in den SFRs;

— andere Begriffe, die durch die Vervollständigung von Operationen in die SFRs und/oder SARs eingeführt werden, wenn diese Begriffe nicht sofort klar sind oder außerhalb ihrer Wörterbuchdefinition verwendet werden.

Ziel dieser Workunit ist es, sicherzustellen, dass die SFRs und SARs klar definiert sind und dass keine Missverständnisse durch die Einführung vager Begriffe entstehen können. Diese Workunit sollte nicht bis zum Äußersten getrieben werden, indem der Verfasser des PP gezwungen wird, jedes einzelne Wort zu definieren. Bei den allgemeinen Adressaten einer Menge Sicherheitsanforderungen sollte davon ausgegangen werden, dass sie über angemessene Kenntnisse der IT, der Sicherheit und der „Evaluierungskriterien für die IT-Sicherheit“ verfügen.

All dies kann in Gruppen, Klassen, Rollen, Typen oder anderen Gruppierungen oder Charakterisierungen dargestellt werden, die ein einfaches Verständnis ermöglichen.

Der Evaluator wird daran erinnert, dass diese Listen und Definitionen nicht Teil der Aussage der Sicherheitsanforderungen sein müssen, sondern (teilweise oder ganz) in verschiedenen Unterabschnitten untergebracht werden können. Dies kann insbesondere dann der Fall sein, wenn die gleichen Begriffe im übrigen PP verwendet werden.

ISO/IEC 15408-3 APE_REQ.1.3C: *Die Aussage zu den Sicherheitsanforderungen muss alle Operationen im Zusammenhang mit den Sicherheitsanforderungen identifizieren.*

8.8.1.3.4 Workunit APE_REQ.1-4

Der Evaluator ***muss prüfen***, ob in der Aussage der Sicherheitsanforderungen alle Operationen zur Erfüllung der Sicherheitsanforderungen aufgeführt sind.

Der Evaluator stellt fest, dass alle Operationen in jeder SFR oder SAR, in denen eine solche Operation verwendet wird, identifiziert werden. Dies umfasst sowohl abgeschlossene als auch nicht abgeschlossene Operationen. Die Identifizierung kann durch typografische Unterscheidungen, durch explizite Kennzeichnung im umgebenden Text oder durch jedes andere Unterscheidungsmittel erfolgen.

ISO/IEC 15408-3 APE_REQ.1.4C: *Alle Operationen müssen korrekt durchgeführt werden.*

8.8.1.3.5 Workunit ASE_REQ.1-5

Der Evaluator ***muss*** die Aussage der Sicherheitsanforderungen ***untersuchen***, um festzustellen, dass alle Zuordnungsoperationen korrekt durchgeführt werden.

Leitlinien zur korrekten Durchführung der Operationen können ISO/IEC 15408-1, Anhang C, Leitlinien für Operationen, entnommen werden.

8.8.1.3.6 Workunit APE_REQ.1-6

Der Evaluator ***muss*** die Aussage der Sicherheitsanforderungen ***untersuchen***, um festzustellen, dass alle Iterationsoperationen korrekt durchgeführt werden.

Leitlinien zur korrekten Durchführung der Operationen können ISO/IEC 15408-1, Anhang C, Leitlinien für Operationen, entnommen werden.

AVA Documents
Document Sharing Hub

Full document details: DIN EN ISO/IEC 18045:2021-02

8.8.1.3.7 Workunit APE_REQ.1-7

Der Evaluator ***muss*** die Aussage der Sicherheitsanforderungen ***untersuchen***, um festzustellen, dass alle Auswahloperationen korrekt durchgeführt werden.

Leitlinien zur korrekten Durchführung der Operationen können ISO/IEC 15408-1, Anhang C, Leitlinien für Operationen, entnommen werden.

8.8.1.3.8 Workunit APE_REQ.1-8

Der Evaluator ***muss*** die Aussage der Sicherheitsanforderungen ***untersuchen***, um festzustellen, dass alle Präzisierungsoperationen korrekt durchgeführt werden.

Leitlinien zur korrekten Durchführung der Operationen können ISO/IEC 15408-1, Anhang C, Leitlinien für Operationen, entnommen werden.

ISO/IEC 15408-3 APE_REQ.1.5C: *Jede Abhängigkeit der Sicherheitsanforderungen muss entweder erfüllt sein, oder die Begründung für die Sicherheitsanforderungen muss rechtfertigen, dass die Abhängigkeit nicht erfüllt wird.*

8.8.1.3.9 Workunit APE_REQ.1-9

Der Evaluator ***muss*** die Aussage der Sicherheitsanforderungen ***untersuchen***, um festzustellen, dass jede Abhängigkeit der Sicherheitsanforderungen entweder erfüllt ist oder ob die Begründung der Sicherheitsanforderungen die Nichterfüllung der Abhängigkeit rechtfertigt.

Eine Abhängigkeit wird durch die Einbeziehung der betreffenden Komponente (oder einer zu ihr hierarchischen Komponente) in die Aussage der Sicherheitsanforderungen erfüllt. Die Komponente, die zur Erfüllung der Abhängigkeit verwendet wird, sollte gegebenenfalls durch Operationen modifiziert werden, um sicherzustellen, dass sie diese Abhängigkeit auch tatsächlich erfüllt.

In einer Begründung, dass eine Abhängigkeit nicht erfüllt ist, sollte ebenfalls angesprochen werden

a) warum die Abhängigkeit nicht erforderlich oder sinnvoll ist, wobei in diesem Fall keine weiteren Informationen erforderlich sind; oder

b) dass die Abhängigkeit über die Betriebsumgebung des TOEs behandelt wurde; in diesem Fall sollte in der Begründung beschrieben sein, wie die Sicherheitszielsetzungen für die Betriebsumgebung diese Abhängigkeit behandeln.

ISO/IEC 15408-3 APE_REQ.1.6C: *Die Aussage zu den Sicherheitsanforderungen muss in sich konsistent sein.*

8.8.1.3.10 Workunit APE_REQ.1-10

Der Evaluator ***muss*** die Aussage der Sicherheitsanforderungen ***untersuchen***, um festzustellen, dass sie in sich konsistent ist.

Der Evaluator stellt fest, dass die kombinierte Menge aller SFRs und SARs in sich konsistent ist.

Der Evaluator stellt fest, dass in allen Fällen, in denen unterschiedliche Sicherheitsanforderungen für die gleichen Arten von Nachweisen, Ereignissen, Operationen, Daten, durchzuführenden Prüfungen usw. für den Entwickler oder für „alle Objekte“, „alle Subjekte“ usw. gelten, diese Anforderungen nicht im Widerspruch zueinander stehen.

Documents
Document Sharing Hub
Full document details: DIN EN ISO/IEC 18045:2021-02