

E DIN EN ISO/IEC 18045:2023-12 (D/E)

Erscheinungsdatum: 2023-11-17

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

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

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

10.3	PP-Einleitung (APE_INT)	33
10.3.1	Evaluierung der Unteraufgabe (APE_INT.1)	33
10.4	Konformitätsansprüche (APE_CCL)	35
10.4.1	Evaluierung der Unteraufgabe (APE_CCL.1)	35
10.5	Sicherheitsproblemdefinition (APE_SPD)	45
10.5.1	Evaluierung der Unteraufgabe (APE_SPD.1)	45
10.6	Sicherheitszielsetzungen (APE_OBJ)	47
10.6.1	Evaluierung der Unteraufgabe (APE_OBJ.1)	47
10.6.2	Evaluierung der Unteraufgabe (APE_OBJ.2)	48
10.7	Erweiterte Komponentendefinition (APE_ECD)	51
10.7.1	Evaluierung der Unteraufgabe (APE_ECD.1)	51
10.8	Sicherheitsanforderungen (APE_REQ)	55
10.8.1	Evaluierung der Unteraufgabe (APE_REQ.1)	55
10.8.2	Evaluierung der Unteraufgabe (APE_REQ.2)	61
11	Klasse ACE: Evaluierung der Schutzprofilkonfiguration	66
11.1	Allgemeines	66
11.2	Einleitung für PP-Module (ACE_INT)	68
11.2.1	Evaluierung der Unteraufgabe (ACE_INT.1)	68
11.3	Konformitätsansprüche des PP-Moduls (ACE_CCL)	70
11.3.1	Evaluierung der Unteraufgabe (ACE_CCL.1)	70
11.4	Sicherheitsproblemdefinition des PP-Moduls (ACE_SPD)	76
11.4.1	Evaluierung der Unteraufgabe (ACE_SPD.1)	76
11.5	Sicherheitszielsetzungen des PP-Moduls (ACE_OBJ)	77
11.5.1	Evaluierung der Unteraufgabe (ACE_OBJ.1)	77
11.5.2	Evaluierung der Unteraufgabe (ACE_OBJ.2)	78
11.6	Erweiterte Komponentendefinition des PP-Moduls (ACE_ECD)	81
11.6.1	Evaluierung der Unteraufgabe (ACE_ECD.1)	81
11.7	Sicherheitsanforderungen des PP-Moduls (ACE_REQ)	85
11.7.1	Evaluierung der Unteraufgabe (ACE_REQ.1)	85
11.7.2	Evaluierung der Unteraufgabe (ACE_REQ.2)	91
11.8	Konsistenz des PP-Moduls (ACE_MCO)	97
11.8.1	Evaluierung der Unteraufgabe (ACE_MCO.1)	97
11.9	Konsistenz der PP-Konfiguration (ACE_CCO)	100
11.9.1	Evaluierung der Unteraufgabe (ACE_CCO.1)	100
12	Klasse ASE: Evaluierung der Sicherheitsvorgabe	109
12.1	Allgemeines	109
12.2	Anwendungshinweise	109
12.2.1	Wiederverwendung der Evaluierungsergebnisse von zertifizierten PPs	109
12.3	ST-Einleitung (ASE_INT)	110
12.3.1	Evaluierung der Unteraufgabe (ASE_INT.1)	110
12.4	Konformitätsansprüche (ASE_CCL)	114
12.4.1	Evaluierung der Unteraufgabe (ASE_CCL.1)	114
12.5	Sicherheitsproblemdefinition (ASE_SPD)	129
12.5.1	Evaluierung der Unteraufgabe (ASE_SPD.1)	129
12.6	Sicherheitszielsetzungen (ASE_OBJ)	131
12.6.1	Evaluierung der Unteraufgabe (ASE_OBJ.1)	131
12.6.2	Evaluierung der Unteraufgabe (ASE_OBJ.2)	132
12.7	Erweiterte Komponentendefinition (ASE_ECD)	135
12.7.1	Evaluierung der Unteraufgabe (ASE_ECD.1)	135
12.8	Sicherheitsanforderungen (ASE_REQ)	139
12.8.1	Evaluierung der Unteraufgabe (ASE_REQ.1)	139
12.8.2	Evaluierung der Unteraufgabe (ASE_REQ.2)	145
12.9	Zusammenfassende Spezifikation des TOE (ASE_TSS)	152
12.9.1	Evaluierung der Unteraufgabe (ASE_TSS.1)	152
12.9.2	Evaluierung der Unteraufgabe (ASE_TSS.2)	153
12.10	Konsistenz der Sicherheitsvorgaben des Verbundprodukts (ASE_COMP)	154
12.10.1	Allgemeines	154

12.10.2	Evaluierung der Unteraufgabe (ASE_COMP.1)	155
13	Klasse ADV: Entwicklung	160
13.1	Allgemeines	160
13.2	Anwendungshinweise	161
13.3	Sicherheitsarchitektur (ADV_ARC)	161
13.3.1	Evaluierung der Unteraufgabe (ADV_ARC.1)	161
13.4	Funktionsspezifikation (ADV_FSP)	167
13.4.1	Evaluierung der Unteraufgabe (ADV_FSP.1)	167
13.4.2	Evaluierung der Unteraufgabe (ADV_FSP.2)	171
13.4.3	Evaluierung der Unteraufgabe (ADV_FSP.3)	176
13.4.4	Evaluierung der Unteraufgabe (ADV_FSP.4)	182
13.4.5	Evaluierung der Unteraufgabe (ADV_FSP.5)	188
13.4.6	Evaluierung der Unteraufgabe (ADV_FSP.6)	195
13.5	Darstellung der Implementierung (ADV_IMP)	195
13.5.1	Evaluierung der Unteraufgabe (ADV_IMP.1)	195
13.5.2	Evaluierung der Unteraufgabe (ADV_IMP.2)	197
13.6	TSF-Interna (ADV_INT)	201
13.6.1	Evaluierung der Unteraufgabe (ADV_INT.1)	201
13.6.2	Evaluierung der Unteraufgabe (ADV_INT.2)	203
13.6.3	Evaluierung der Unteraufgabe (ADV_INT.3)	206
13.7	Formales TSF-Modell (ADV_SPM)	209
13.7.1	Evaluierung der Unteraufgabe (ADV_SPM.1)	209
13.8	TOE-Design (ADV_TDS)	216
13.8.1	Evaluierung der Unteraufgabe (ADV_TDS.1)	216
13.8.2	Evaluierung der Unteraufgabe (ADV_TDS.2)	220
13.8.3	Evaluierung der Unteraufgabe (ADV_TDS.3)	226
13.8.4	Evaluierung der Unteraufgabe (ADV_TDS.4)	236
13.8.5	Evaluierung der Unteraufgabe (ADV_TDS.5)	246
13.8.6	Evaluierung der Unteraufgabe (ADV_TDS.6)	255
13.9	Konformität mit dem zusammengesetzten Design (ADV_COMP)	256
13.9.1	Allgemeines	256
13.9.2	Evaluierung der Unteraufgabe (ADV_COMP.1)	256
14	Klasse AGD: Leitliniendokumente	258
14.1	Allgemeines	258
14.2	Anwendungshinweise	258
14.3	Operative Leitlinien für Benutzer (AGD_OPE)	259
14.3.1	Evaluierung der Unteraufgabe (AGD_OPE.1)	259
14.4	Vorbereitende Verfahren (AGD_PRE)	262
14.4.1	Evaluierung der Unteraufgabe (AGD_PRE.1)	262
15	Klasse ALC: Unterstützung des Lebenszyklus	264
15.1	Allgemeines	264
15.2	CM-Funktionen (ALC_CMC)	265
15.2.1	Evaluierung der Unteraufgabe (ALC_CMC.1)	265
15.2.2	Evaluierung der Unteraufgabe (ALC_CMC.2)	266
15.2.3	Evaluierung der Unteraufgabe (ALC_CMC.3)	268
15.2.4	Evaluierung der Unteraufgabe (ALC_CMC.4)	272
15.2.5	Evaluierung der Unteraufgabe (ALC_CMC.5)	278
15.3	CM-Umfang (ALC_CMS)	286
15.3.1	Evaluierung der Unteraufgabe (ALC_CMS.1)	286
15.3.2	Evaluierung der Unteraufgabe (ALC_CMS.2)	287
15.3.3	Evaluierung der Unteraufgabe (ALC_CMS.3)	288
15.3.4	Evaluierung der Unteraufgabe (ALC_CMS.4)	289
15.3.5	Evaluierung der Unteraufgabe (ALC_CMS.5)	290
15.4	Lieferung (ALC_DEL)	292
15.4.1	Evaluierung der Unteraufgabe (ALC_DEL.1)	292
15.5	Entwicklungssicherheit (ALC_DVS)	293

15.5.1	Evaluierung der Unteraufgabe (ALC_DVS.1)	293
15.5.2	Evaluierung der Unteraufgabe (ALC_DVS.2)	296
15.6	Mängelbeseitigung (ALC_FLR)	299
15.6.1	Evaluierung der Unteraufgabe (ALC_FLR.1)	299
15.6.2	Evaluierung der Unteraufgabe (ALC_FLR.2)	302
15.6.3	Evaluierung der Unteraufgabe (ALC_FLR.3)	306
15.7	Definition des Lebenszyklus (ALC_LCD)	312
15.7.1	Evaluierung der Unteraufgabe (ALC_LCD.1)	312
15.7.2	Evaluierung der Unteraufgabe (ALC_LCD.2)	313
15.8	Artefakte der TOE-Entwicklung (ALC_TDA)	315
15.8.1	Evaluierung der Unteraufgabe (ALC_TDA.1)	315
15.8.2	Evaluierung der Unteraufgabe (ALC_TDA.2)	319
15.8.3	Evaluierung der Unteraufgabe (ALC_TDA.3)	322
15.9	Tools und Techniken (ALC_TAT)	327
15.9.1	Evaluierung der Unteraufgabe (ALC_TAT.1)	327
15.9.2	Evaluierung der Unteraufgabe (ALC_TAT.2)	329
15.9.3	Evaluierung der Unteraufgabe (ALC_TAT.3)	332
15.10	Integration von Zusammensetzungsteilen und Konsistenzprüfung von Lieferverfahren (ALC_COMP)	336
15.10.1	Allgemeines	336
15.10.2	Evaluierung der Unteraufgabe (ALC_COMP.1)	336
16	Klasse ATE: Prüfungen	339
16.1	Allgemeines	339
16.2	Anwendungshinweise	339
16.2.1	Verständnis des erwarteten Verhaltens des TOE	340
16.2.2	Prüfen gegenüber alternativen Ansätzen zur Überprüfung des erwarteten Verhaltens der Funktionalität	340
16.2.3	Überprüfung der Angemessenheit der Prüfungen	340
16.3	Abdeckung (ATE_COV)	341
16.3.1	Evaluierung der Unteraufgabe (ATE_COV.1)	341
16.3.2	Evaluierung der Unteraufgabe (ATE_COV.2)	342
16.3.3	Evaluierung der Unteraufgabe (ATE_COV.3)	343
16.4	Tiefe (ATE_DPT)	345
16.4.1	Evaluierung der Unteraufgabe (ATE_DPT.1)	345
16.4.2	Evaluierung der Unteraufgabe (ATE_DPT.2)	348
16.4.3	Evaluierung der Unteraufgabe (ATE_DPT.3)	351
16.4.4	Evaluierung der Unteraufgabe (ATE_DPT.4)	354
16.5	Funktionsprüfungen (ATE_FUN)	354
16.5.1	Evaluierung der Unteraufgabe (ATE_FUN.1)	354
16.5.2	Evaluierung der Unteraufgabe (ATE_FUN.2)	357
16.6	Unabhängiges Prüfen (ATE_IND)	362
16.6.1	Evaluierung der Unteraufgabe (ATE_IND.1)	362
16.6.2	Evaluierung der Unteraufgabe (ATE_IND.2)	366
16.6.3	Evaluierung der Unteraufgabe (ATE_IND.3)	372
16.7	Zusammengesetzte Funktionsprüfung (ATE_COMP)	372
16.7.1	Allgemeines	372
16.7.2	Evaluierung der Unteraufgabe (ATE_COMP.1)	372
17	Klasse AVA: Anfälligkeitsbewertung	374
17.1	Allgemeines	374
17.2	Anfälligkeitsanalyse (AVA_VAN)	374
17.2.1	Evaluierung der Unteraufgabe (AVA_VAN.1)	374
17.2.2	Evaluierung der Unteraufgabe (AVA_VAN.2)	380
17.2.3	Evaluierung der Unteraufgabe (AVA_VAN.3)	387
17.2.4	Evaluierung der Unteraufgabe (AVA_VAN.4)	397
17.2.5	Evaluierung der Unteraufgabe (AVA_VAN.5)	405
17.3	Zusammengesetzte Anfälligkeitsbewertung (AVA_COMP)	413
17.3.1	Allgemeines	413

17.3.2	Evaluierung der Unteraufgabe (AVA_COMP.1)	413
18	Klasse ACO: Zusammensetzung	416
18.1	Allgemeines	416
18.2	Anwendungshinweise	416
18.3	Begründung der Zusammensetzung (ACO_COR)	417
18.3.1	Evaluierung der Unteraufgabe (ACO_COR.1)	417
18.4	Entwicklungsnachweis (ACO_DEV)	424
18.4.1	Evaluierung der Unteraufgabe (ACO_DEV.1)	424
18.4.2	Evaluierung der Unteraufgabe (ACO_DEV.2)	425
18.4.3	Evaluierung der Unteraufgabe (ACO_DEV.3)	427
18.5	Verlässlichkeit der abhängigen Komponente (ACO_REL)	430
18.5.1	Evaluierung der Unteraufgabe (ACO_REL.1)	430
18.5.2	Evaluierung der Unteraufgabe (ACO_REL.2)	432
18.6	Prüfen des zusammengesetzten TOE (ACO_CTT)	435
18.6.1	Evaluierung der Unteraufgabe (ACO_CTT.1)	435
18.6.2	Evaluierung der Unteraufgabe (ACO_CTT.2)	438
18.7	Anfälligkeitsanalyse der Zusammensetzung (ACO_VUL)	441
18.7.1	Evaluierung der Unteraufgabe (ACO_VUL.1)	441
18.7.2	Anwendungshinweise	442
18.7.3	Evaluierung der Unteraufgabe (ACO_VUL.2)	445
18.7.4	Evaluierung der Unteraufgabe (ACO_VUL.3)	449
Anhang A (informativ) Allgemeine Evaluierungsleitlinien		453
A.1	Zielsetzungen	453
A.2	Probenahme	453
A.3	Abhängigkeiten	455
A.3.1	Allgemeines	455
A.3.2	Abhängigkeiten zwischen Aufgaben	455
A.3.3	Abhängigkeiten zwischen Unteraufgaben	455
A.3.4	Abhängigkeiten zwischen Aktionen	456
A.4	Ortsbegehungen	456
A.4.1	Allgemeines	456
A.4.2	Allgemeiner Ansatz	457
A.5	Orientierungshilfe für die Erstellung der Checkliste	457
A.5.1	Aspekte des Konfigurationsmanagements	458
A.5.2	Aspekte der Entwicklungssicherheit	458
A.5.3	Beispiel für eine Checkliste	459
A.6	Zuständigkeiten des Systems	461
Anhang B (informativ) Anfälligkeitsbewertung (AVA)		463
B.1	Was bedeutet Anfälligkeitsanalyse	463
B.2	Erstellung einer Anfälligkeitsanalyse durch den Evaluator	464
B.3	Allgemeine Leitlinien für Anfälligkeiten	464
B.3.1	Umgehen	464
B.3.2	Manipulation	466
B.3.3	Direkte Angriffe	469
B.3.4	Überwachung	470
B.3.5	Fehlbenutzung	471
B.4	Identifizierung potentieller Anfälligkeiten	472
B.4.1	Erkennen	472
B.4.2	Analyse	473
B.5	Bei Verwendung des Angriffspotentials	475
B.5.1	Entwickler	475
B.5.2	Evaluator	476
B.6	Berechnung des Angriffspotentials	477
B.6.1	Anwendung des Angriffspotentials	477
B.6.2	Charakterisierung des Angriffspotentials	478
B.7	Beispielrechnung für einen direkten Angriff	485

Anhang C (informativ) Evaluierungstechniken und -Tools.....	487
C.1 Semiformale und formale Verfahren.....	487
C.1.1 Allgemeines.....	487
C.1.2 Beschreibung der Stile.....	487