ISO/IEC 18045:2026-05 (E)

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Requirements and methodology for IT security evaluation

Contents

Page

Foreword ... viii

Introduction ... ix

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 1

4 Terminology ... 4

5 Verb usage ... 5

6 General evaluation guidance ... 5

7 Relationship between structures within the CC and the structure of this document ... 5

8 Evaluation process and related tasks ... 6

8.1 General ... 6

8.2 Evaluation process overview ... 6

8.2.1 Objectives ... 6

8.2.2 Responsibilities of the roles ... 6

8.2.3 Relationship of roles ... 7

8.2.4 General evaluation model ... 7

8.2.5 Evaluator verdicts ... 8

8.3 Evaluation input task ... 9

8.3.1 Objectives ... 9

8.3.2 Application notes ... 9

8.3.3 Management of evaluation evidence task ... 10

8.4 Evaluation sub-activities ... 11

8.5 Evaluation output task ... 11

8.5.1 Objectives ... 11

8.5.2 Management of evaluation outputs ... 11

8.5.3 Application notes ... 11

8.5.4 Write OR task ... 11

8.5.5 Write ETR task ... 12

9 Protection Profile (PP) evaluation ... 19

9.1 Introduction ... 19

9.2 Application notes ... 19

9.2.1 Re-using the evaluation results of certified PPs ... 19

9.3 PP introduction (APE_INT) ... 20

9.3.1 Evaluation of sub-activity (APE_INT.1) ... 20

9.4 Conformance claims (APE_CCL) ... 21

9.4.1 Evaluation of sub-activity (APE_CCL.1) ... 21

9.5 Security problem definition (APE_SPD) ... 32

9.5.1 Evaluation of sub-activity (APE_SPD.1) ... 32

9.6 Security objectives (APE_OBJ) ... 33

9.6.1 Evaluation of sub-activity (APE_OBJ.1) ... 33

9.6.2 Evaluation of sub-activity (APE_OBJ.2) ... 35

9.7 Extended components definition (APE_ECD) ... 37

9.7.1 Evaluation of sub-activity (APE_ECD.1) ... 37

9.8 Security requirements (APE_REQ) ... 41

9.8.1 Evaluation of sub-activity (APE_REQ.1) ... 41

9.8.2 Evaluation of sub-activity (APE_REQ.2) ... 47

10 Protection Profile Configuration evaluation 51
10.1 Introduction 51
10.2 PP-Module introduction (ACE_INT) 52
10.2.1 Evaluation of sub-activity (ACE_INT.1) 52
10.3 PP-Module conformance claims (ACE_CCL) 55
10.3.1 Evaluation of sub-activity (ACE_CCL.1) 55
10.4 PP-Module security problem definition (ACE_SPD) 61
10.4.1 Evaluation of sub-activity (ACE_SPD.1) 61
10.5 PP-Module security objectives (ACE_OBJ) 62
10.5.1 Evaluation of sub-activity (ACE_OBJ.1) 62
10.5.2 Evaluation of sub-activity (ACE_OBJ.2) 64
10.6 PP-Module extended components definition (ACE_ECD) 66
10.6.1 Evaluation of sub-activity (ACE_ECD.1) 66
10.7 PP-Module security requirements (ACE_REQ) 70
10.7.1 Evaluation of sub-activity (ACE_REQ.1) 70
10.7.2 Evaluation of sub-activity (ACE_REQ.2) 76
10.8 PP-Module consistency (ACE_MCO) 81
10.8.1 Evaluation of sub-activity (ACE_MCO.1) 81
10.9 PP-Configuration consistency (ACE_CCO) 84
10.9.1 Evaluation of sub-activity (ACE_CCO.1) 84

11 Security Target (ST) evaluation 93
11.1 Introduction 93
11.2 Application notes 93
11.2.1 Re-using the evaluation results of certified PPs 93
11.2.2 Composition 94
11.3 ST introduction (ASE_INT) 94
11.3.1 Evaluation of sub-activity (ASE_INT.1) 94
11.4 Conformance claims (ASE_CCL) 98
11.4.1 Evaluation of sub-activity (ASE_CCL.1) 98
11.5 Security problem definition (ASE_SPD) 112
11.5.1 Evaluation of sub-activity (ASE_SPD.1) 112
11.6 Security objectives (ASE_OBJ) 113
11.6.1 Evaluation of sub-activity (ASE_OBJ.1) 113
11.6.2 Evaluation of sub-activity (ASE_OBJ.2) 115
11.7 Extended components definition (ASE_ECD) 117
11.7.1 Evaluation of sub-activity (ASE_ECD.1) 117
11.8 Security requirements (ASE_REQ) 121
11.8.1 Evaluation of sub-activity (ASE_REQ.1) 121
11.8.2 Evaluation of sub-activity (ASE_REQ.2) 128
11.9 TOE summary specification (ASE_TSS) 134
11.9.1 Evaluation of sub-activity (ASE_TSS.1) 134
11.9.2 Evaluation of sub-activity (ASE_TSS.2) 135
11.10 Consistency of composite product Security Target (ASE_COMP) 136
11.10.1 Evaluation of sub-activity (ASE_COMP.1) 136

12 Development 141
12.1 Introduction 141
12.2 Application notes 141
12.2.1 General 141
12.2.2 Composition 142
12.3 Security architecture (ADV_ARC) 142
12.3.1 Evaluation of sub-activity (ADV_ARC.1) 142
12.4 Functional specification (ADV_FSP) 147
12.4.1 Evaluation of sub-activity (ADV_FSP.1) 147
12.4.2 Evaluation of sub-activity (ADV_FSP.2) 150
12.4.3 Evaluation of sub-activity (ADV_FSP.3) 155
12.4.4 Evaluation of sub-activity (ADV_FSP.4) 160
12.4.5 Evaluation of sub-activity (ADV_FSP.5) 166
12.5 Implementation representation (ADV_IMP) 172
12.5.1 Evaluation of sub-activity (ADV_IMP.1) 172
12.5.2 Evaluation of sub-activity (ADV_IMP.2) 174
12.6 TSF internals (ADV_INT) 177
12.6.1 Evaluation of sub-activity (ADV_INT.1) 177
12.6.2 Evaluation of sub-activity (ADV_INT.2) 180

12.6.3 Evaluation of sub-activity (ADV_INT.3) 182
12.7 Formal TSF model (ADV_SPM) 185
12.7.1 Evaluation of sub-activity (ADV_SPM.1) 185
12.8 TOE design (ADV_TDS) 191
12.8.1 Evaluation of sub-activity (ADV_TDS.1) 191
12.8.2 Evaluation of sub-activity (ADV_TDS.2) 195
12.8.3 Evaluation of sub-activity (ADV_TDS.3) 200
12.8.4 Evaluation of sub-activity (ADV_TDS.4) 209
12.8.5 Evaluation of sub-activity (ADV_TDS.5) 219
12.9 Composite design compliance (ADV_COMP) 227
12.9.1 Evaluation of sub-activity (ADV_COMP.1) 227

13 Guidance documents 229
13.1 Introduction 229
13.2 Application notes 229
13.3 Operational user guidance (AGD_OPE) 230
13.3.1 Evaluation of sub-activity (AGD_OPE.1) 230
13.4 Preparative procedures (AGD_PRE) 233
13.4.1 Evaluation of sub-activity (AGD_PRE.1) 233

14 life cycle support 235
14.1 Introduction 235
14.2 Application notes 235
14.2.1 Composition 235
14.3 CM capabilities (ALC_CMC) 236
14.3.1 Evaluation of sub-activity (ALC_CMC.1) 236
14.3.2 Evaluation of sub-activity (ALC_CMC.2) 237
14.3.3 Evaluation of sub-activity (ALC_CMC.3) 239
14.3.4 Evaluation of sub-activity (ALC_CMC.4) 243
14.3.5 Evaluation of sub-activity (ALC_CMC.5) 248
14.4 CM scope (ALC_CMS) 256
14.4.1 Evaluation of sub-activity (ALC_CMS.1) 256
14.4.2 Evaluation of sub-activity (ALC_CMS.2) 257
14.4.3 Evaluation of sub-activity (ALC_CMS.3) 258
14.4.4 Evaluation of sub-activity (ALC_CMS.4) 259
14.4.5 Evaluation of sub-activity (ALC_CMS.5) 260
14.5 Delivery (ALC_DEL) 262
14.5.1 Evaluation of sub-activity (ALC_DEL.1) 262
14.6 Developer environment security (ALC_DVS) 263
14.6.1 Evaluation of sub-activity (ALC_DVS.1) 263
14.6.2 Evaluation of sub-activity (ALC_DVS.2) 265
14.7 Flaw remediation (ALC_FLR) 268
14.7.1 Evaluation of sub-activity (ALC_FLR.1) 268
14.7.2 Evaluation of sub-activity (ALC_FLR.2) 271
14.7.3 Evaluation of sub-activity (ALC_FLR.3) 274
14.8 Development life cycle definition (ALC_LCD) 280
14.8.1 Evaluation of sub-activity (ALC_LCD.1) 280
14.8.2 Evaluation of sub-activity (ALC_LCD.2) 281
14.9 TOE development artefacts (ALC_TDA) 284
14.9.1 Evaluation of sub-activity (ALC_TDA.1) 284
14.9.2 Evaluation of sub-activity (ALC_TDA.2) 287
14.9.3 Evaluation of sub-activity (ALC_TDA.3) 291
14.10 Tools and techniques (ALC_TAT) 296
14.10.1 Evaluation of sub-activity (ALC_TAT.1) 296
14.10.2 Evaluation of sub-activity (ALC_TAT.2) 298
14.10.3 Evaluation of sub-activity (ALC_TAT.3) 301
14.11 Integration of composition parts and consistency check of delivery procedures (ALC_COMP) 304
14.11.1 Evaluation of sub-activity (ALC_COMP.1) 304

15 Tests **306**
15.1 Introduction 306
15.2 Application notes 307
15.2.1 General 307
15.2.2 Understanding the expected behaviour of the TOE 307
15.2.3 Testing vs. alternate approaches to verify the expected behaviour of functionality 307
15.2.4 Verifying the adequacy of tests 308
15.2.5 Composition 308
15.3 Coverage (ATE_COV) 309
15.3.1 Evaluation of sub-activity (ATE_COV.1) 309
15.3.2 Evaluation of sub-activity (ATE_COV.2) 309
15.3.3 Evaluation of sub-activity (ATE_COV.3) 311
15.4 Depth (ATE_DPT) 313
15.4.1 Evaluation of sub-activity (ATE_DPT.1) 313
15.4.2 Evaluation of sub-activity (ATE_DPT.2) 315
15.4.3 Evaluation of sub-activity (ATE_DPT.3) 318
15.5 Functional tests (ATE_FUN) 321
15.5.1 Evaluation of sub-activity (ATE_FUN.1) 321
15.5.2 Evaluation of sub-activity (ATE_FUN.2) 324
15.6 Independent testing (ATE_IND) 328
15.6.1 Evaluation of sub-activity (ATE_IND.1) 328
15.6.2 Evaluation of sub-activity (ATE_IND.2) 331
15.7 Composite functional testing (ATE_COMP) 336
15.7.1 Evaluation of sub-activity (ATE_COMP.1) 336

16 Vulnerability assessment **338**
16.1 Introduction 338
16.2 Application notes 338
16.2.1 Composition 338
16.3 Vulnerability analysis (AVA_VAN) 338
16.3.1 Evaluation of sub-activity (AVA_VAN.1) 338
16.3.2 Evaluation of sub-activity (AVA_VAN.2) 344
16.3.3 Evaluation of sub-activity (AVA_VAN.3) 351
16.3.4 Evaluation of sub-activity (AVA_VAN.4) 359
16.3.5 Evaluation of sub-activity (AVA_VAN.5) 367
16.4 Composite vulnerability assessment (AVA_COMP) 375
16.4.1 Evaluation of sub-activity (AVA_COMP.1) 375

17 Composition **378**
17.1 Introduction 378
17.2 Application notes 378
17.3 Composition rationale (ACO_COR) 379
17.3.1 Evaluation of sub-activity (ACO_COR.1) 379
17.4 Development evidence (ACO_DEV) 385
17.4.1 Evaluation of sub-activity (ACO_DEV.1) 385
17.4.2 Evaluation of sub-activity (ACO_DEV.2) 387
17.4.3 Evaluation of sub-activity (ACO_DEV.3) 389
17.5 Reliance of dependent component (ACO_REL) 391
17.5.1 Evaluation of sub-activity (ACO_REL.1) 391
17.5.2 Evaluation of sub-activity (ACO_REL.2) 394
17.6 Composed TOE testing (ACO_CTT) 396
17.6.1 Evaluation of sub-activity (ACO_CTT.1) 396
17.6.2 Evaluation of sub-activity (ACO_CTT.2) 399
17.7 Composition vulnerability analysis (ACO_VUL) 403
17.7.1 Evaluation of sub-activity (ACO_VUL.1) 403
17.7.2 Evaluation of sub-activity (ACO_VUL.2) 406
17.7.3 Evaluation of sub-activity (ACO_VUL.3) 410

Annex A (informative) **General evaluation guidance and requirements** **415**

Annex B (normative) **Vulnerability assessment (AVA)** **423**
Annex C (informative) **Evaluation techniques and tools - Semi-formal and formal methods** **443**
Bibliography **447**