

# ISO/IEC 18045:2022-08 (E)

## Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Methodology for IT security evaluation

---

### Contents

	Page
LIST OF FIGURES .....	ix
LIST OF TABLES .....	x
FOREWORD .....	xi
INTRODUCTION .....	xii
<b>1 SCOPE .....</b>	<b>1</b>
<b>2 NORMATIVE REFERENCES .....</b>	<b>1</b>
<b>3 TERMS AND DEFINITIONS .....</b>	<b>1</b>
<b>4 ABBREVIATED TERMS .....</b>	<b>4</b>
<b>5 TERMINOLOGY .....</b>	<b>4</b>
<b>6 VERB USAGE .....</b>	<b>4</b>
<b>7 GENERAL EVALUATION GUIDANCE.....</b>	<b>5</b>
<b>8 RELATIONSHIP BETWEEN THE ISO/IEC 15408 SERIES AND ISO/IEC 18045 STRUCTURES.....</b>	<b>5</b>
<b>9 EVALUATION PROCESS AND RELATED TASKS .....</b>	<b>5</b>
9.1 GENERAL .....	5
9.2 EVALUATION PROCESS OVERVIEW .....	6
9.2.1 Objectives.....	6
9.2.2 Responsibilities of the roles .....	6
9.2.3 Relationship of roles .....	6
9.2.4 General evaluation model .....	7
9.2.5 Evaluator verdicts.....	7
9.3 EVALUATION INPUT TASK.....	9
9.3.1 Objectives.....	9
9.3.2 Application notes.....	9
9.3.3 Management of evaluation evidence sub-task.....	10
9.4 EVALUATION SUB-ACTIVITIES.....	10
9.5 EVALUATION OUTPUT TASK .....	10
9.5.1 Objectives.....	10
9.5.2 Management of evaluation outputs.....	11
9.5.3 Application notes.....	11
9.5.4 Write OR sub-task.....	11
9.5.5 Write ETR sub-task.....	11
<b>10 CLASS APE: PROTECTION PROFILE EVALUATION.....</b>	<b>19</b>
10.1 GENERAL .....	19
10.2 RE-USING THE EVALUATION RESULTS OF CERTIFIED PPS .....	19
10.3 PP INTRODUCTION (APE_INT) .....	20
10.3.1 Evaluation of sub-activity (APE_INT.1).....	20
10.4 CONFORMANCE CLAIMS (APE_CCL).....	21
10.4.1 Evaluation of sub-activity (APE_CCL.1).....	21
10.5 SECURITY PROBLEM DEFINITION (APE_SPD).....	31
10.5.1 Evaluation of sub-activity (APE_SPD.1) .....	31
10.6 SECURITY OBJECTIVES (APE_OBJ).....	32
10.6.1 Evaluation of sub-activity (APE_OBJ.1).....	32
10.6.2 Evaluation of sub-activity (APE_OBJ.2).....	33
10.7 EXTENDED COMPONENTS DEFINITION (APE_ECD).....	36
10.7.1 Evaluation of sub-activity (APE_ECD.1).....	36

10.8	SECURITY REQUIREMENTS (APE_REQ)	40
10.8.1	<i>Evaluation of sub-activity (APE_REQ.1)</i>	40
10.8.2	<i>Evaluation of sub-activity (APE_REQ.2)</i>	45
<b>11</b>	<b>CLASS ACE: PROTECTION PROFILE CONFIGURATION EVALUATION</b>	<b>49</b>
11.1	GENERAL	49
11.2	PP-MODULE INTRODUCTION (ACE_INT)	51
11.2.1	<i>Evaluation of sub-activity (ACE_INT.1)</i>	51
11.3	PP-MODULE CONFORMANCE CLAIMS (ACE_CCL)	53
11.3.1	<i>Evaluation of sub-activity (ACE_CCL.1)</i>	53
11.4	PP-MODULE SECURITY PROBLEM DEFINITION (ACE_SPD)	58
11.4.1	<i>Evaluation of sub-activity (ACE_SPD.1)</i>	58
11.5	PP-MODULE SECURITY OBJECTIVES (ACE_OBJ)	59
11.5.1	<i>Evaluation of sub-activity (ACE_OBJ.1)</i>	59
11.5.2	<i>Evaluation of sub-activity (ACE_OBJ.2)</i>	60
11.6	PP-MODULE EXTENDED COMPONENTS DEFINITION (ACE_ECD)	63
11.6.1	<i>Evaluation of sub-activity (ACE_ECD.1)</i>	63
11.7	PP-MODULE SECURITY REQUIREMENTS (ACE_REQ)	67
11.7.1	<i>Evaluation of sub-activity (ACE_REQ.1)</i>	67
11.7.2	<i>Evaluation of sub-activity (ACE_REQ.2)</i>	72
11.8	PP-MODULE CONSISTENCY (ACE_MCO)	76
11.8.1	<i>Evaluation of sub-activity (ACE_MCO.1)</i>	76
11.9	PP-CONFIGURATION CONSISTENCY (ACE_CCO)	79
11.9.1	<i>Evaluation of sub-activity (ACE_CCO.1)</i>	79
<b>12</b>	<b>CLASS ASE: SECURITY TARGET EVALUATION</b>	<b>87</b>
12.1	GENERAL	87
12.2	APPLICATION NOTES	87
12.2.1	<i>Re-using the evaluation results of certified PPs</i>	87
12.3	ST INTRODUCTION (ASE_INT)	88
12.3.1	<i>Evaluation of sub-activity (ASE_INT.1)</i>	88
12.4	CONFORMANCE CLAIMS (ASE_CCL)	91
12.4.1	<i>Evaluation of sub-activity (ASE_CCL.1)</i>	91
12.5	SECURITY PROBLEM DEFINITION (ASE_SPD)	105
12.5.1	<i>Evaluation of sub-activity (ASE_SPD.1)</i>	105
12.6	SECURITY OBJECTIVES (ASE_OBJ)	106
12.6.1	<i>Evaluation of sub-activity (ASE_OBJ.1)</i>	106
12.6.2	<i>Evaluation of sub-activity (ASE_OBJ.2)</i>	107
12.7	EXTENDED COMPONENTS DEFINITION (ASE_ECD)	109
12.7.1	<i>Evaluation of sub-activity (ASE_ECD.1)</i>	109
12.8	SECURITY REQUIREMENTS (ASE_REQ)	113
12.8.1	<i>Evaluation of sub-activity (ASE_REQ.1)</i>	113
12.8.2	<i>Evaluation of sub-activity (ASE_REQ.2)</i>	119
12.9	TOE SUMMARY SPECIFICATION (ASE_TSS)	124
12.9.1	<i>Evaluation of sub-activity (ASE_TSS.1)</i>	124
12.9.2	<i>Evaluation of sub-activity (ASE_TSS.2)</i>	125
12.10	CONSISTENCY OF COMPOSITE PRODUCT SECURITY TARGET (ASE_COMP)	127
12.10.1	<i>General</i>	127
12.10.2	<i>Evaluation of sub-activity (ASE_COMP.1)</i>	127
<b>13</b>	<b>CLASS ADV: DEVELOPMENT</b>	<b>132</b>
13.1	GENERAL	132
13.2	APPLICATION NOTES	132
13.3	SECURITY ARCHITECTURE (ADV_ARC)	133
13.3.1	<i>Evaluation of sub-activity (ADV_ARC.1)</i>	133
13.4	FUNCTIONAL SPECIFICATION (ADV_FSP)	137
13.4.1	<i>Evaluation of sub-activity (ADV_FSP.1)</i>	137
13.4.2	<i>Evaluation of sub-activity (ADV_FSP.2)</i>	140

13.4.3	Evaluation of sub-activity (ADV_FSP.3)	145
13.4.4	Evaluation of sub-activity (ADV_FSP.4)	150
13.4.5	Evaluation of sub-activity (ADV_FSP.5)	155
13.4.6	Evaluation of sub-activity (ADV_FSP.6)	161
13.5	IMPLEMENTATION REPRESENTATION (ADV_IMP)	161
13.5.1	Evaluation of sub-activity (ADV_IMP.1)	161
13.5.2	Evaluation of sub-activity (ADV_IMP.2)	164
13.6	TSF INTERNALS (ADV_INT)	166
13.6.1	Evaluation of sub-activity (ADV_INT.1)	166
13.6.2	Evaluation of sub-activity (ADV_INT.2)	169
13.6.3	Evaluation of sub-activity (ADV_INT.3)	171
13.7	FORMAL TSF MODEL (ADV_SPM)	173
13.7.1	Evaluation of sub-activity (ADV_SPM.1)	173
13.8	TOE DESIGN (ADV_TDS)	180
13.8.1	Evaluation of sub-activity (ADV_TDS.1)	180
13.8.2	Evaluation of sub-activity (ADV_TDS.2)	183
13.8.3	Evaluation of sub-activity (ADV_TDS.3)	188
13.8.4	Evaluation of sub-activity (ADV_TDS.4)	197
13.8.5	Evaluation of sub-activity (ADV_TDS.5)	206
13.8.6	Evaluation of sub-activity (ADV_TDS.6)	213
13.9	COMPOSITE DESIGN COMPLIANCE (ADV_COMP)	214
13.9.1	General	214
13.9.2	Evaluation of sub-activity (ADV_COMP.1)	214
<b>14</b>	<b>CLASS AGD: GUIDANCE DOCUMENTS</b>	<b>216</b>
14.1	GENERAL	216
14.2	APPLICATION NOTES	216
14.3	OPERATIONAL USER GUIDANCE (AGD_OPE)	216
14.3.1	Evaluation of sub-activity (AGD_OPE.1)	216
14.4	PREPARATIVE PROCEDURES (AGD_PRE)	219
14.4.1	Evaluation of sub-activity (AGD_PRE.1)	219
<b>15</b>	<b>CLASS ALC: LIFE-CYCLE SUPPORT</b>	<b>221</b>
15.1	GENERAL	221
15.2	CM CAPABILITIES (ALC_CMC)	222
15.2.1	Evaluation of sub-activity (ALC_CMC.1)	222
15.2.2	Evaluation of sub-activity (ALC_CMC.2)	223
15.2.3	Evaluation of sub-activity (ALC_CMC.3)	224
15.2.4	Evaluation of sub-activity (ALC_CMC.4)	228
15.2.5	Evaluation of sub-activity (ALC_CMC.5)	233
15.3	CM SCOPE (ALC_CMS)	240
15.3.1	Evaluation of sub-activity (ALC_CMS.1)	240
15.3.2	Evaluation of sub-activity (ALC_CMS.2)	241
15.3.3	Evaluation of sub-activity (ALC_CMS.3)	242
15.3.4	Evaluation of sub-activity (ALC_CMS.4)	243
15.3.5	Evaluation of sub-activity (ALC_CMS.5)	244
15.4	DELIVERY (ALC_DEL)	245
15.4.1	Evaluation of sub-activity (ALC_DEL.1)	245
15.5	DEVELOPMENT SECURITY (ALC_DVS)	247
15.5.1	Evaluation of sub-activity (ALC_DVS.1)	247
15.5.2	Evaluation of sub-activity (ALC_DVS.2)	249
15.6	FLAW REMEDIATION (ALC_FLR)	252
15.6.1	Evaluation of sub-activity (ALC_FLR.1)	252
15.6.2	Evaluation of sub-activity (ALC_FLR.2)	254
15.6.3	Evaluation of sub-activity (ALC_FLR.3)	257
15.7	LIFE-CYCLE DEFINITION (ALC_LCD)	262
15.7.1	Evaluation of sub-activity (ALC_LCD.1)	262
15.7.2	Evaluation of sub-activity (ALC_LCD.2)	263

15.8	TOE DEVELOPMENT ARTIFACTS (ALC_TDA).....	265
15.8.1	<i>Evaluation of sub-activity (ALC_TDA.1)</i> .....	265
15.8.2	<i>Evaluation of sub-activity (ALC_TDA.2)</i> .....	268
15.8.3	<i>Evaluation of sub-activity (ALC_TDA.3)</i> .....	272
15.9	TOOLS AND TECHNIQUES (ALC_TAT).....	276
15.9.1	<i>Evaluation of sub-activity (ALC_TAT.1)</i> .....	276
15.9.2	<i>Evaluation of sub-activity (ALC_TAT.2)</i> .....	278
15.9.3	<i>Evaluation of sub-activity (ALC_TAT.3)</i> .....	281
15.10	INTEGRATION OF COMPOSITION PARTS AND CONSISTENCY CHECK OF DELIVERY PROCEDURES (ALC_COMP).....	284
15.10.1	<i>General</i> .....	284
15.10.2	<i>Evaluation of sub-activity (ALC_COMP.1)</i> .....	284
<b>16</b>	<b>CLASS ATE: TESTS.....</b>	<b>286</b>
16.1	GENERAL.....	286
16.2	APPLICATION NOTES.....	287
16.2.1	<i>Understanding the expected behaviour of the TOE</i> .....	287
16.2.2	<i>Testing vs. alternate approaches to verify the expected behaviour of functionality</i> .....	288
16.2.3	<i>Verifying the adequacy of tests</i> .....	288
16.3	COVERAGE (ATE_COV).....	288
16.3.1	<i>Evaluation of sub-activity (ATE_COV.1)</i> .....	288
16.3.2	<i>Evaluation of sub-activity (ATE_COV.2)</i> .....	289
16.3.3	<i>Evaluation of sub-activity (ATE_COV.3)</i> .....	291
16.4	DEPTH (ATE_DPT).....	293
16.4.1	<i>Evaluation of sub-activity (ATE_DPT.1)</i> .....	293
16.4.2	<i>Evaluation of sub-activity (ATE_DPT.2)</i> .....	295
16.4.3	<i>Evaluation of sub-activity (ATE_DPT.3)</i> .....	298
16.4.4	<i>Evaluation of sub-activity (ATE_DPT.4)</i> .....	300
16.5	FUNCTIONAL TESTS (ATE_FUN).....	300
16.5.1	<i>Evaluation of sub-activity (ATE_FUN.1)</i> .....	300
16.5.2	<i>Evaluation of sub-activity (ATE_FUN.2)</i> .....	303
16.6	INDEPENDENT TESTING (ATE_IND).....	307
16.6.1	<i>Evaluation of sub-activity (ATE_IND.1)</i> .....	307
16.6.2	<i>Evaluation of sub-activity (ATE_IND.2)</i> .....	311
16.6.3	<i>Evaluation of sub-activity (ATE_IND.3)</i> .....	316
16.7	COMPOSITE FUNCTIONAL TESTING (ATE_COMP).....	316
16.7.1	<i>General</i> .....	316
16.7.2	<i>Evaluation of sub-activity (ATE_COMP.1)</i> .....	316
<b>17</b>	<b>CLASS AVA: VULNERABILITY ASSESSMENT.....</b>	<b>317</b>
17.1	GENERAL.....	317
17.2	VULNERABILITY ANALYSIS (AVA_VAN).....	318
17.2.1	<i>Evaluation of sub-activity (AVA_VAN.1)</i> .....	318
17.2.2	<i>Evaluation of sub-activity (AVA_VAN.2)</i> .....	323
17.2.3	<i>Evaluation of sub-activity (AVA_VAN.3)</i> .....	329
17.2.4	<i>Evaluation of sub-activity (AVA_VAN.4)</i> .....	337
17.2.5	<i>Evaluation of sub-activity (AVA_VAN.5)</i> .....	345
17.3	COMPOSITE VULNERABILITY ASSESSMENT (AVA_COMP).....	352
17.3.1	<i>General</i> .....	352
17.3.2	<i>Evaluation of sub-activity (AVA_COMP.1)</i> .....	352
<b>18</b>	<b>CLASS ACO: COMPOSITION.....</b>	<b>354</b>
18.1	GENERAL.....	354
18.2	APPLICATION NOTES.....	354
18.3	COMPOSITION RATIONALE (ACO_COR).....	355
18.3.1	<i>Evaluation of sub-activity (ACO_COR.1)</i> .....	355
18.4	DEVELOPMENT EVIDENCE (ACO_DEV).....	362
18.4.1	<i>Evaluation of sub-activity (ACO_DEV.1)</i> .....	362
18.4.2	<i>Evaluation of sub-activity (ACO_DEV.2)</i> .....	363

18.4.3	<i>Evaluation of sub-activity (ACO_DEV.3)</i> .....	365
18.5	RELIANCE OF DEPENDENT COMPONENT (ACO_REL).....	368
18.5.1	<i>Evaluation of sub-activity (ACO_REL.1)</i> .....	368
18.5.2	<i>Evaluation of sub-activity (ACO_REL.2)</i> .....	370
18.6	COMPOSED TOE TESTING (ACO_CTT).....	372
18.6.1	<i>Evaluation of sub-activity (ACO_CTT.1)</i> .....	372
18.6.2	<i>Evaluation of sub-activity (ACO_CTT.2)</i> .....	375
18.7	COMPOSITION VULNERABILITY ANALYSIS (ACO_VUL).....	378
18.7.1	<i>Evaluation of sub-activity (ACO_VUL.1)</i> .....	378
18.7.2	<i>Application notes</i> .....	378
18.7.3	<i>Evaluation of sub-activity (ACO_VUL.2)</i> .....	381
18.7.4	<i>Evaluation of sub-activity (ACO_VUL.3)</i> .....	384
<b>ANNEX A (INFORMATIVE) GENERAL EVALUATION GUIDANCE</b> .....		<b>389</b>
<b>A.1</b>	<b>OBJECTIVES</b> .....	<b>389</b>
<b>A.2</b>	<b>SAMPLING</b> .....	<b>389</b>
<b>A.3</b>	<b>DEPENDENCIES</b> .....	<b>391</b>
<b>A.3.1</b>	<b>GENERAL</b> .....	<b>391</b>
<b>A.3.2</b>	<b>DEPENDENCIES BETWEEN ACTIVITIES</b> .....	<b>391</b>
<b>A.3.3</b>	<b>DEPENDENCIES BETWEEN SUB-ACTIVITIES</b> .....	<b>391</b>
<b>A.3.4</b>	<b>DEPENDENCIES BETWEEN ACTIONS</b> .....	<b>391</b>
<b>A.4</b>	<b>SITE VISITS</b> .....	<b>391</b>
<b>A.4.1</b>	<b>GENERAL</b> .....	<b>391</b>
<b>A.4.2</b>	<b>GENERAL APPROACH</b> .....	<b>392</b>
<b>A.5</b>	<b>ORIENTATION GUIDE FOR THE PREPARATION OF THE CHECKLIST</b> .....	<b>393</b>
<b>A.5.1</b>	<b>ASPECTS OF CONFIGURATION MANAGEMENT</b> .....	<b>393</b>
<b>A.5.2</b>	<b>ASPECTS OF DEVELOPMENT SECURITY</b> .....	<b>393</b>
<b>A.5.3</b>	<b>EXAMPLE OF A CHECKLIST</b> .....	<b>394</b>
<b>A.6</b>	<b>SCHEME RESPONSIBILITIES</b> .....	<b>397</b>
<b>ANNEX B (INFORMATIVE) VULNERABILITY ASSESSMENT (AVA)</b> .....		<b>399</b>
<b>B.1</b>	<b>WHAT IS VULNERABILITY ANALYSIS</b> .....	<b>399</b>
<b>B.2</b>	<b>EVALUATOR CONSTRUCTION OF A VULNERABILITY ANALYSIS</b> .....	<b>399</b>
<b>B.3</b>	<b>GENERIC VULNERABILITY GUIDANCE</b> .....	<b>400</b>
<b>B.3.1</b>	<b>BYPASSING</b> .....	<b>400</b>
<b>B.3.2</b>	<b>TAMPERING</b> .....	<b>402</b>
<b>B.3.3</b>	<b>DIRECT ATTACKS</b> .....	<b>405</b>
<b>B.3.4</b>	<b>MONITORING</b> .....	<b>405</b>
<b>B.3.5</b>	<b>MISUSE</b> .....	<b>406</b>
<b>B.4</b>	<b>IDENTIFICATION OF POTENTIAL VULNERABILITIES</b> .....	<b>407</b>
<b>B.4.1</b>	<b>ENCOUNTERED</b> .....	<b>407</b>
<b>B.4.2</b>	<b>ANALYSIS</b> .....	<b>408</b>
<b>B.4.2.1</b>	<b>GENERAL</b> .....	<b>408</b>
<b>B.4.2.2</b>	<b>UNSTRUCTURED ANALYSIS</b> .....	<b>408</b>

<b>B.4.2.3</b>	<b>FOCUSED</b> .....	<b>408</b>
<b>B.4.2.4</b>	<b>METHODICAL</b> .....	<b>409</b>
<b>B.5</b>	<b>WHEN ATTACK POTENTIAL IS USED</b> .....	<b>410</b>
<b>B.5.1</b>	<b>DEVELOPER</b> .....	<b>410</b>
<b>B.5.2</b>	<b>EVALUATOR</b> .....	<b>410</b>
<b>B.6</b>	<b>CALCULATING ATTACK POTENTIAL</b> .....	<b>411</b>
<b>B.6.1</b>	<b>APPLICATION OF ATTACK POTENTIAL</b> .....	<b>411</b>
<b>B.6.1.1</b>	<b>GENERAL</b> .....	<b>411</b>
<b>B.6.1.2</b>	<b>TREATMENT OF MOTIVATION</b> .....	<b>411</b>
<b>B.6.2</b>	<b>CHARACTERISING ATTACK POTENTIAL</b> .....	<b>412</b>
<b>B.6.2.1</b>	<b>GENERAL</b> .....	<b>412</b>
<b>B.6.2.2</b>	<b>DETERMINING THE ATTACK POTENTIAL</b> .....	<b>412</b>
<b>B.6.2.3</b>	<b>FACTORS TO BE CONSIDERED</b> .....	<b>412</b>
<b>B.6.2.4</b>	<b>CALCULATION OF ATTACK POTENTIAL</b> .....	<b>415</b>
<b>B.7</b>	<b>EXAMPLE CALCULATION FOR DIRECT ATTACK</b> .....	<b>418</b>
	<b>ANNEX C (INFORMATIVE) EVALUATION TECHNIQUES AND TOOLS</b> .....	<b>420</b>
<b>C.1</b>	<b>SEMIFORMAL AND FORMAL METHODS</b> .....	<b>420</b>
<b>C.1.1</b>	<b>GENERAL</b> .....	<b>420</b>
<b>C.1.2</b>	<b>DESCRIPTION OF STYLES</b> .....	<b>420</b>
<b>C.1.2.1</b>	<b>INFORMAL STYLE</b> .....	<b>421</b>
<b>C.1.2.2</b>	<b>SEMIFORMAL STYLE</b> .....	<b>422</b>
<b>C.1.2.3</b>	<b>FORMAL STYLE</b> .....	<b>423</b>

## List of figures

FIGURE 1 — MAPPING OF THE ISO/IEC 15408 SERIES AND ISO/IEC 18045 STRUCTURES.....	5
FIGURE 2 — GENERIC EVALUATION MODEL.....	7
FIGURE 3 — EXAMPLE OF THE VERDICT ASSIGNMENT RULE.....	8
FIGURE 4 — ETR INFORMATION CONTENT FOR A PP EVALUATION.....	12
FIGURE 5 — ETR INFORMATION CONTENT FOR A PP-CONFIGURATION EVALUATION.....	14
FIGURE 6 — ETR INFORMATION CONTENT FOR A TOE EVALUATION.....	17
FIGURE 7 — RELATIONSHIP BETWEEN PPS AND PP-MODULES IN A PP-CONFIGURATION.....	50
FIGURE 8 — EXAMPLE OF EXACT CONFORMANCE RELATIONSHIPS BETWEEN AN ST AND PPS.....	94

## List of tables

TABLE 1 — ASE_COMP.....	127
TABLE 2 — ADV_COMP.....	214
TABLE 3 — ALC_COMP.....	284
TABLE 4 — ATE_COMP.....	316
TABLE 5 — AVA_COMP.....	352
TABLE A.1 — EXAMPLE OF A CHECKLIST AT EAL 4 (EXTRACT).....	395
TABLE B.1 — VULNERABILITY TESTING AND ATTACK POTENTIAL.....	410
TABLE B.2 — CALCULATION OF ATTACK POTENTIAL.....	415
TABLE B.3 — RATING OF VULNERABILITIES AND TOE RESISTANCE.....	417