

# DIN EN ISO/IEC 18045:2021-02 (E)

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

---

<b>Contents</b>		<b>Page</b>
European foreword .....		6
Foreword .....		7
Introduction .....		9
<b>1</b>	<b>Scope .....</b>	<b>10</b>
<b>2</b>	<b>Normative references .....</b>	<b>10</b>
<b>3</b>	<b>Terms and definitions .....</b>	<b>10</b>
<b>4</b>	<b>Symbols and abbreviated terms .....</b>	<b>12</b>
<b>5</b>	<b>Overview .....</b>	<b>12</b>
<b>5.1</b>	<b>Organisation of this International Standard .....</b>	<b>12</b>
<b>6</b>	<b>Document Conventions .....</b>	<b>12</b>
<b>6.1</b>	<b>Terminology .....</b>	<b>12</b>
<b>6.2</b>	<b>Verb usage .....</b>	<b>12</b>
<b>6.3</b>	<b>General evaluation guidance .....</b>	<b>13</b>
<b>6.4</b>	<b>Relationship between ISO/IEC 15408 and ISO/IEC 18045 structures .....</b>	<b>13</b>
<b>7</b>	<b>Evaluation process and related tasks .....</b>	<b>14</b>
<b>7.1</b>	<b>Introduction .....</b>	<b>14</b>
<b>7.2</b>	<b>Evaluation process overview .....</b>	<b>14</b>
<b>7.2.1</b>	<b>Objectives .....</b>	<b>14</b>
<b>7.2.2</b>	<b>Responsibilities of the roles .....</b>	<b>14</b>
<b>7.2.3</b>	<b>Relationship of roles .....</b>	<b>15</b>
<b>7.2.4</b>	<b>General evaluation model .....</b>	<b>15</b>
<b>7.2.5</b>	<b>Evaluator verdicts .....</b>	<b>15</b>
<b>7.3</b>	<b>Evaluation input task .....</b>	<b>17</b>
<b>7.3.1</b>	<b>Objectives .....</b>	<b>17</b>
<b>7.3.2</b>	<b>Application notes .....</b>	<b>17</b>
<b>7.3.3</b>	<b>Management of evaluation evidence sub-task .....</b>	<b>17</b>
<b>7.4</b>	<b>Evaluation sub-activities .....</b>	<b>18</b>
<b>7.5</b>	<b>Evaluation output task .....</b>	<b>18</b>
<b>7.5.1</b>	<b>Objectives .....</b>	<b>18</b>
<b>7.5.2</b>	<b>Management of evaluation outputs .....</b>	<b>18</b>
<b>7.5.3</b>	<b>Application notes .....</b>	<b>19</b>
<b>7.5.4</b>	<b>Write OR sub-task .....</b>	<b>19</b>
<b>7.5.5</b>	<b>Write ETR sub-task .....</b>	<b>19</b>
<b>8</b>	<b>Class APE: Protection Profile evaluation .....</b>	<b>24</b>
<b>8.1</b>	<b>Introduction .....</b>	<b>24</b>
<b>8.2</b>	<b>Application notes .....</b>	<b>25</b>
<b>8.2.1</b>	<b>Re-using the evaluation results of certified PPs .....</b>	<b>25</b>
<b>8.3</b>	<b>PP introduction (APE_INT) .....</b>	<b>25</b>
<b>8.3.1</b>	<b>Evaluation of sub-activity (APE_INT.1) .....</b>	<b>25</b>
<b>8.4</b>	<b>Conformance claims (APE_CCL) .....</b>	<b>26</b>
<b>8.4.1</b>	<b>Evaluation of sub-activity (APE_CCL.1) .....</b>	<b>26</b>

8.5	Security problem definition (APE_SPD) .....	33
8.5.1	Evaluation of sub-activity (APE_SPD.1) .....	33
8.6	Security objectives (APE_OBJ) .....	34
8.6.1	Evaluation of sub-activity (APE_OBJ.1) .....	34
8.6.2	Evaluation of sub-activity (APE_OBJ.2) .....	34
8.7	Extended components definition (APE_ECD) .....	37
8.7.1	Evaluation of sub-activity (APE_ECD.1) .....	37
8.8	Security requirements (APE_REQ) .....	40
8.8.1	Evaluation of sub-activity (APE_REQ.1) .....	40
8.8.2	Evaluation of sub-activity (APE_REQ.2) .....	44
<b>9</b>	<b>Class ASE: Security Target evaluation .....</b>	<b>48</b>
9.1	Introduction .....	48
9.2	Application notes .....	48
9.2.1	Re-using the evaluation results of certified PPs .....	48
9.3	ST introduction (ASE_INT) .....	48
9.3.1	Evaluation of sub-activity (ASE_INT.1) .....	48
9.4	Conformance claims (ASE_CCL) .....	51
9.4.1	Evaluation of sub-activity (ASE_CCL.1) .....	51
9.5	Security problem definition (ASE_SPD) .....	58
9.5.1	Evaluation of sub-activity (ASE_SPD.1) .....	58
9.6	Security objectives (ASE_OBJ) .....	60
9.6.1	Evaluation of sub-activity (ASE_OBJ.1) .....	60
9.6.2	Evaluation of sub-activity (ASE_OBJ.2) .....	60
9.7	Extended components definition (ASE_ECD) .....	62
9.7.1	Evaluation of sub-activity (ASE_ECD.1) .....	62
9.8	Security requirements (ASE_REQ) .....	66
9.8.1	Evaluation of sub-activity (ASE_REQ.1) .....	66
9.8.2	Evaluation of sub-activity (ASE_REQ.2) .....	69
9.9	TOE summary specification (ASE_TSS) .....	73
9.9.1	Evaluation of sub-activity (ASE_TSS.1) .....	73
9.9.2	Evaluation of sub-activity (ASE_TSS.2) .....	74
<b>10</b>	<b>Class ADV: Development .....</b>	<b>76</b>
10.1	Introduction .....	76
10.2	Application notes .....	76
10.3	Security Architecture (ADV_ARC) .....	76
10.3.1	Evaluation of sub-activity (ADV_ARC.1) .....	76
10.4	Functional specification (ADV_FSP) .....	81
10.4.1	Evaluation of sub-activity (ADV_FSP.1) .....	81
10.4.2	Evaluation of sub-activity (ADV_FSP.2) .....	84
10.4.3	Evaluation of sub-activity (ADV_FSP.3) .....	88
10.4.4	Evaluation of sub-activity (ADV_FSP.4) .....	93
10.4.5	Evaluation of sub-activity (ADV_FSP.5) .....	98
10.4.6	Evaluation of sub-activity (ADV_FSP.6) .....	103
10.5	Implementation representation (ADV_IMP) .....	104
10.5.1	Evaluation of sub-activity (ADV_IMP.1) .....	104
10.5.2	Evaluation of sub-activity (ADV_IMP.2) .....	106
10.6	TSF internals (ADV_INT) .....	106
10.6.1	Evaluation of sub-activity (ADV_INT.1) .....	106
10.6.2	Evaluation of sub-activity (ADV_INT.2) .....	108
10.6.3	Evaluation of sub-activity (ADV_INT.3) .....	110
10.7	Security policy modelling (ADV_SPM) .....	110
10.7.1	Evaluation of sub-activity (ADV_SPM.1) .....	110
10.8	TOE design (ADV_TDS) .....	110
10.8.1	Evaluation of sub-activity (ADV_TDS.1) .....	110
10.8.2	Evaluation of sub-activity (ADV_TDS.2) .....	114
10.8.3	Evaluation of sub-activity (ADV_TDS.3) .....	118
10.8.4	Evaluation of sub-activity (ADV_TDS.4) .....	127
10.8.5	Evaluation of sub-activity (ADV_TDS.5) .....	135
10.8.6	Evaluation of sub-activity (ADV_TDS.6) .....	135

<b>11</b>	<b>Class AGD: Guidance documents</b> .....	<b>136</b>
11.1	Introduction .....	136
11.2	Application notes .....	136
11.3	Operational user guidance (AGD_OPE) .....	136
11.3.1	Evaluation of sub-activity (AGD_OPE.1) .....	136
11.4	Preparative procedures (AGD_PRE) .....	139
11.4.1	Evaluation of sub-activity (AGD_PRE.1) .....	139
<b>12</b>	<b>Class ALC: Life-cycle support</b> .....	<b>140</b>
12.1	Introduction .....	140
12.2	CM capabilities (ALC_CMC) .....	141
12.2.1	Evaluation of sub-activity (ALC_CMC.1) .....	141
12.2.2	Evaluation of sub-activity (ALC_CMC.2) .....	142
12.2.3	Evaluation of sub-activity (ALC_CMC.3) .....	144
12.2.4	Evaluation of sub-activity (ALC_CMC.4) .....	147
12.2.5	Evaluation of sub-activity (ALC_CMC.5) .....	152
12.3	CM scope (ALC_CMS) .....	159
12.3.1	Evaluation of sub-activity (ALC_CMS.1) .....	159
12.3.2	Evaluation of sub-activity (ALC_CMS.2) .....	160
12.3.3	Evaluation of sub-activity (ALC_CMS.3) .....	161
12.3.4	Evaluation of sub-activity (ALC_CMS.4) .....	162
12.3.5	Evaluation of sub-activity (ALC_CMS.5) .....	163
12.4	Delivery (ALC_DEL) .....	164
12.4.1	Evaluation of sub-activity (ALC_DEL.1) .....	164
12.5	Development security (ALC_DVS) .....	165
12.5.1	Evaluation of sub-activity (ALC_DVS.1) .....	165
12.5.2	Evaluation of sub-activity (ALC_DVS.2) .....	167
12.6	Flaw remediation (ALC_FLR) .....	170
12.6.1	Evaluation of sub-activity (ALC_FLR.1) .....	170
12.6.2	Evaluation of sub-activity (ALC_FLR.2) .....	172
12.6.3	Evaluation of sub-activity (ALC_FLR.3) .....	176
12.7	Life-cycle definition (ALC_LCD) .....	180
12.7.1	Evaluation of sub-activity (ALC_LCD.1) .....	180
12.7.2	Evaluation of sub-activity (ALC_LCD.2) .....	181
12.8	Tools and techniques (ALC_TAT) .....	183
12.8.1	Evaluation of sub-activity (ALC_TAT.1) .....	183
12.8.2	Evaluation of sub-activity (ALC_TAT.2) .....	185
12.8.3	Evaluation of sub-activity (ALC_TAT.3) .....	187
<b>13</b>	<b>Class ATE: Tests</b> .....	<b>190</b>
13.1	Introduction .....	190
13.2	Application notes .....	190
13.2.1	Understanding the expected behaviour of the TOE .....	190
13.2.2	Testing vs. alternate approaches to verify the expected behaviour of functionality .....	191
13.2.3	Verifying the adequacy of tests .....	191
13.3	Coverage (ATE_COV) .....	192
13.3.1	Evaluation of sub-activity (ATE_COV.1) .....	192
13.3.2	Evaluation of sub-activity (ATE_COV.2) .....	192
13.3.3	Evaluation of sub-activity (ATE_COV.3) .....	193
13.4	Depth (ATE_DPT) .....	194
13.4.1	Evaluation of sub-activity (ATE_DPT.1) .....	194
13.4.2	Evaluation of sub-activity (ATE_DPT.2) .....	196
13.4.3	Evaluation of sub-activity (ATE_DPT.3) .....	198
13.4.4	Evaluation of sub-activity (ATE_DPT.4) .....	201
13.5	Functional tests (ATE_FUN) .....	201
13.5.1	Evaluation of sub-activity (ATE_FUN.1) .....	201
13.5.2	Evaluation of sub-activity (ATE_FUN.2) .....	204
13.6	Independent testing (ATE_IND) .....	204
13.6.1	Evaluation of sub-activity (ATE_IND.1) .....	204
13.6.2	Evaluation of sub-activity (ATE_IND.2) .....	207
13.6.3	Evaluation of sub-activity (ATE_IND.3) .....	212

<b>14</b>	<b>Class AVA: Vulnerability assessment</b> .....	<b>212</b>
14.1	Introduction .....	212
14.2	Vulnerability analysis (AVA_VAN) .....	213
14.2.1	Evaluation of sub-activity (AVA_VAN.1) .....	213
14.2.2	Evaluation of sub-activity (AVA_VAN.2) .....	217
14.2.3	Evaluation of sub-activity (AVA_VAN.3) .....	224
14.2.4	Evaluation of sub-activity (AVA_VAN.4) .....	231
14.2.5	Evaluation of sub-activity (AVA_VAN.5) .....	239
<b>15</b>	<b>Class ACO: Composition</b> .....	<b>239</b>
15.1	Introduction .....	239
15.2	Application notes .....	239
15.3	Composition rationale (ACO_COR) .....	240
15.3.1	Evaluation of sub-activity (ACO_COR.1) .....	240
15.4	Development evidence (ACO_DEV) .....	245
15.4.1	Evaluation of sub-activity (ACO_DEV.1) .....	245
15.4.2	Evaluation of sub-activity (ACO_DEV.2) .....	246
15.4.3	Evaluation of sub-activity (ACO_DEV.3) .....	248
15.5	Reliance of dependent component (ACO_REL) .....	251
15.5.1	Evaluation of sub-activity (ACO_REL.1) .....	251
15.5.2	Evaluation of sub-activity (ACO_REL.2) .....	253
15.6	Composed TOE testing (ACO_CTT) .....	255
15.6.1	Evaluation of sub-activity (ACO_CTT.1) .....	255
15.6.2	Evaluation of sub-activity (ACO_CTT.2) .....	257
15.7	Composition vulnerability analysis (ACO_VUL) .....	261
15.7.1	Evaluation of sub-activity (ACO_VUL.1) .....	261
15.7.2	Evaluation of sub-activity (ACO_VUL.2) .....	263
15.7.3	Evaluation of sub-activity (ACO_VUL.3) .....	267
<b>Annex A (informative) General evaluation guidance</b> .....	<b>271</b>	
A.1	Objectives .....	271
A.2	Sampling .....	271
A.3	Dependencies .....	273
A.3.1	Dependencies between activities .....	273
A.3.2	Dependencies between sub-activities .....	273
A.3.3	Dependencies between actions .....	273
A.4	Site Visits .....	273
A.4.1	Introduction .....	273
A.4.2	General Approach .....	274
A.4.3	Orientation Guide for the Preparation of the Check List .....	275
A.4.4	Example of a checklist .....	276
A.5	Scheme Responsibilities .....	278
<b>Annex B (informative) Vulnerability Assessment (AVA)</b> .....	<b>280</b>	
B.1	What is Vulnerability Analysis .....	280
B.2	Evaluator construction of a Vulnerability Analysis .....	280
B.2.1	Generic vulnerability guidance .....	281
B.2.2	Identification of Potential Vulnerabilities .....	288
B.3	When attack potential is used .....	290
B.3.1	Developer .....	290
B.3.2	Evaluator .....	291
B.4	Calculating attack potential .....	292
B.4.1	Application of attack potential .....	292
B.4.2	Characterising attack potential .....	292
B.5	Example calculation for direct attack .....	298