

DIN EN ISO/IEC 15408-3:2021-06 (E)

Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components (ISO/IEC 15408-3:2008, Corrected version 2011-06-01)

Contents		Page
European foreword		8
Foreword		9
Introduction		11
1	Scope	12
2	Normative references	12
3	Terms and definitions, symbols and abbreviated terms	12
4	Overview	12
4.1	Organisation of this part of ISO/IEC 15408	12
5	Assurance paradigm	13
5.1	ISO/IEC 15408 philosophy	13
5.2	Assurance approach	13
5.2.1	Significance of vulnerabilities	13
5.2.2	Cause of vulnerabilities	14
5.2.3	ISO/IEC 15408 assurance	14
5.2.4	Assurance through evaluation	14
5.3	ISO/IEC 15408 evaluation assurance scale	14
6	Security assurance components	15
6.1	Security assurance classes, families and components structure	15
6.1.1	Assurance class structure	15
6.1.2	Assurance family structure	16
6.1.3	Assurance component structure	17
6.1.4	Assurance elements	19
6.1.5	Component taxonomy	19
6.2	EAL structure	20
6.2.1	EAL name	20
6.2.2	Objectives	20
6.2.3	Application notes	20
6.2.4	Assurance components	21
6.2.5	Relationship between assurances and assurance levels	21
6.3	CAP structure	22
6.3.1	CAP name	22
6.3.2	Objectives	22
6.3.3	Application notes	22
6.3.4	Assurance components	23
6.3.5	Relationship between assurances and assurance levels	24
7	Evaluation assurance levels	24
7.1	Evaluation assurance level (EAL) overview	25
7.2	Evaluation assurance level details	26
7.3	Evaluation assurance level 1 (EAL1) - functionally tested	26
7.3.1	Objectives	26

7.3.2	Assurance components	27
7.4	Evaluation assurance level 2 (EAL2) - structurally tested	27
7.4.1	Objectives	27
7.4.2	Assurance components	27
7.5	Evaluation assurance level 3 (EAL3) - methodically tested and checked	28
7.5.1	Objectives	28
7.5.2	Assurance components	28
7.6	Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed	29
7.6.1	Objectives	29
7.6.2	Assurance components	29
7.7	Evaluation assurance level 5 (EAL5) - semiformally designed and tested	30
7.7.1	Objectives	30
7.7.2	Assurance components	30
7.8	Evaluation assurance level 6 (EAL6) - semiformally verified design and tested	31
7.8.1	Objectives	31
7.8.2	Assurance components	31
7.9	Evaluation assurance level 7 (EAL7) - formally verified design and tested	32
7.9.1	Objectives	32
7.9.2	Assurance components	33
8	Composed assurance packages	34
8.1	Composed assurance package (CAP) overview	34
8.2	Composed assurance package details	35
8.3	Composition assurance level A (CAP-A) - Structurally composed	35
8.3.1	Objectives	35
8.3.2	Assurance components	35
8.4	Composition assurance level B (CAP-B) - Methodically composed	36
8.4.1	Objectives	36
8.4.2	Assurance components	36
8.5	Composition assurance level C (CAP-C) - Methodically composed, tested and reviewed	37
8.5.1	Objectives	37
8.5.2	Assurance components	37
9	Class APE: Protection Profile evaluation	38
9.1	PP introduction (APE_INT)	39
9.1.1	Objectives	39
9.1.2	APE_INT.1 PP introduction	39
9.2	Conformance claims (APE_CCL)	40
9.2.1	Objectives	40
9.2.2	APE_CCL.1 Conformance claims	40
9.3	Security problem definition (APE_SPD)	42
9.3.1	Objectives	42
9.3.2	APE_SPD.1 Security problem definition	42
9.4	Security objectives (APE_OBJ)	42
9.4.1	Objectives	42
9.4.2	Component levelling	43
9.4.3	APE_OBJ.1 Security objectives for the operational environment	43
9.4.4	APE_OBJ.2 Security objectives	43
9.5	Extended components definition (APE_ECD)	44
9.5.1	Objectives	44
9.5.2	APE_ECD.1 Extended components definition	44
9.6	Security requirements (APE_REQ)	45
9.6.1	Objectives	45
9.6.2	Component levelling	45
9.6.3	APE_REQ.1 Stated security requirements	45
9.6.4	APE_REQ.2 Derived security requirements	46
10	Class ASE: Security Target evaluation	47
10.1	ST introduction (ASE_INT)	48
10.1.1	Objectives	48
10.1.2	ASE_INT.1 ST introduction	48
10.2	Conformance claims (ASE_CCL)	49

10.2.1	Objectives	49
10.2.2	ASE_CCL.1 Conformance claims	49
10.3	Security problem definition (ASE_SPD)	51
10.3.1	Objectives	51
10.3.2	ASE_SPD.1 Security problem definition	51
10.4	Security objectives (ASE_OBJ)	52
10.4.1	Objectives	52
10.4.2	Component levelling	52
10.4.3	ASE_OBJ.1 Security objectives for the operational environment	52
10.4.4	ASE_OBJ.2 Security objectives	52
10.5	Extended components definition (ASE_ECD)	53
10.5.1	Objectives	53
10.5.2	ASE_ECD.1 Extended components definition	53
10.6	Security requirements (ASE_REQ)	54
10.6.1	Objectives	54
10.6.2	Component levelling	54
10.6.3	ASE_REQ.1 Stated security requirements	55
10.6.4	ASE_REQ.2 Derived security requirements	55
10.7	TOE summary specification (ASE_TSS)	57
10.7.1	Objectives	57
10.7.2	Component levelling	57
10.7.3	ASE_TSS.1 TOE summary specification	57
10.7.4	ASE_TSS.2 TOE summary specification with architectural design summary	58
11	Class ADV: Development	59
11.1	Security Architecture (ADV_ARC)	63
11.1.1	Objectives	63
11.1.2	Component levelling	63
11.1.3	Application notes	63
11.1.4	ADV_ARC.1 Security architecture description	64
11.2	Functional specification (ADV_FSP)	65
11.2.1	Objectives	65
11.2.2	Component levelling	65
11.2.3	Application notes	65
11.2.4	ADV_FSP.1 Basic functional specification	67
11.2.5	ADV_FSP.2 Security-enforcing functional specification	68
11.2.6	ADV_FSP.3 Functional specification with complete summary	69
11.2.7	ADV_FSP.4 Complete functional specification	70
11.2.8	ADV_FSP.5 Complete semi-formal functional specification with additional error information	71
11.2.9	ADV_FSP.6 Complete semi-formal functional specification with additional formal specification	72
11.3	Implementation representation (ADV_IMP)	74
11.3.1	Objectives	74
11.3.2	Component levelling	74
11.3.3	Application notes	74
11.3.4	ADV_IMP.1 Implementation representation of the TSF	75
11.3.5	ADV_IMP.2 Complete mapping of the implementation representation of the TSF	75
11.4	TSF internals (ADV_INT)	76
11.4.1	Objectives	76
11.4.2	Component levelling	76
11.4.3	Application notes	76
11.4.4	ADV_INT.1 Well-structured subset of TSF internals	77
11.4.5	ADV_INT.2 Well-structured internals	78
11.4.6	ADV_INT.3 Minimally complex internals	79
11.5	Security policy modelling (ADV_SPM)	80
11.5.1	Objectives	80
11.5.2	Component levelling	80
11.5.3	Application notes	80
11.5.4	ADV_SPM.1 Formal TOE security policy model	81
11.6	TOE design (ADV_TDS)	82
11.6.1	Objectives	82

11.6.2	Component levelling	82
11.6.3	Application notes	82
11.6.4	ADV_TDS.1 Basic design	83
11.6.5	ADV_TDS.2 Architectural design	84
11.6.6	ADV_TDS.3 Basic modular design	85
11.6.7	ADV_TDS.4 Semiformal modular design	87
11.6.8	ADV_TDS.5 Complete semiformal modular design	88
11.6.9	ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation	89
12	Class AGD: Guidance documents	91
12.1	Operational user guidance (AGD_OPE)	91
12.1.1	Objectives	91
12.1.2	Component levelling	92
12.1.3	Application notes	92
12.1.4	AGD_OPE.1 Operational user guidance	92
12.2	Preparative procedures (AGD_PRE)	93
12.2.1	Objectives	93
12.2.2	Component levelling	93
12.2.3	Application notes	93
12.2.4	AGD_PRE.1 Preparative procedures	94
13	Class ALC: Life-cycle support	94
13.1	CM capabilities (ALC_CMC)	95
13.1.1	Objectives	95
13.1.2	Component levelling	96
13.1.3	Application notes	96
13.1.4	ALC_CMC.1 Labelling of the TOE	96
13.1.5	ALC_CMC.2 Use of a CM system	97
13.1.6	ALC_CMC.3 Authorisation controls	98
13.1.7	ALC_CMC.4 Production support, acceptance procedures and automation	99
13.1.8	ALC_CMC.5 Advanced support	101
13.2	CM scope (ALC_CMS)	103
13.2.1	Objectives	103
13.2.2	Component levelling	104
13.2.3	Application notes	104
13.2.4	ALC_CMS.1 TOE CM coverage	104
13.2.5	ALC_CMS.2 Parts of the TOE CM coverage	104
13.2.6	ALC_CMS.3 Implementation representation CM coverage	105
13.2.7	ALC_CMS.4 Problem tracking CM coverage	106
13.2.8	ALC_CMS.5 Development tools CM coverage	107
13.3	Delivery (ALC_DEL)	108
13.3.1	Objectives	108
13.3.2	Component levelling	108
13.3.3	Application notes	108
13.3.4	ALC_DEL.1 Delivery procedures	109
13.4	Development security (ALC_DVS)	109
13.4.1	Objectives	109
13.4.2	Component levelling	109
13.4.3	Application notes	109
13.4.4	ALC_DVS.1 Identification of security measures	110
13.4.5	ALC_DVS.2 Sufficiency of security measures	110
13.5	Flaw remediation (ALC_FLR)	111
13.5.1	Objectives	111
13.5.2	Component levelling	111
13.5.3	Application notes	111
13.5.4	ALC_FLR.1 Basic flaw remediation	111
13.5.5	ALC_FLR.2 Flaw reporting procedures	112
13.5.6	ALC_FLR.3 Systematic flaw remediation	113
13.6	Life-cycle definition (ALC_LCD)	115
13.6.1	Objectives	115
13.6.2	Component levelling	115

13.6.3	Application notes	115
13.6.4	ALC_LCD.1 Developer defined life-cycle model	116
13.6.5	ALC_LCD.2 Measurable life-cycle model	117
13.7	Tools and techniques (ALC_TAT)	117
13.7.1	Objectives	117
13.7.2	Component levelling	118
13.7.3	Application notes	118
13.7.4	ALC_TAT.1 Well-defined development tools	118
13.7.5	ALC_TAT.2 Compliance with implementation standards	119
13.7.6	ALC_TAT.3 Compliance with implementation standards - all parts	119
14	Class ATE: Tests	120
14.1	Coverage (ATE_COV)	121
14.1.1	Objectives	121
14.1.2	Component levelling	121
14.1.3	Application notes	121
14.1.4	ATE_COV.1 Evidence of coverage	121
14.1.5	ATE_COV.2 Analysis of coverage	122
14.1.6	ATE_COV.3 Rigorous analysis of coverage	123
14.2	Depth (ATE_DPT)	123
14.2.1	Objectives	123
14.2.2	Component levelling	124
14.2.3	Application notes	124
14.2.4	ATE_DPT.1 Testing: basic design	124
14.2.5	ATE_DPT.2 Testing: security enforcing modules	125
14.2.6	ATE_DPT.3 Testing: modular design	125
14.2.7	ATE_DPT.4 Testing: implementation representation	126
14.3	Functional tests (ATE_FUN)	127
14.3.1	Objectives	127
14.3.2	Component levelling	127
14.3.3	Application notes	127
14.3.4	ATE_FUN.1 Functional testing	128
14.3.5	ATE_FUN.2 Ordered functional testing	128
14.4	Independent testing (ATE_IND)	129
14.4.1	Objectives	129
14.4.2	Component levelling	129
14.4.3	Application notes	130
14.4.4	ATE_IND.1 Independent testing - conformance	130
14.4.5	ATE_IND.2 Independent testing - sample	131
14.4.6	ATE_IND.3 Independent testing - complete	132
15	Class AVA: Vulnerability assessment	133
15.1	Application notes	133
15.2	Vulnerability analysis (AVA_VAN)	134
15.2.1	Objectives	134
15.2.2	Component levelling	134
15.2.3	AVA_VAN.1 Vulnerability survey	134
15.2.4	AVA_VAN.2 Vulnerability analysis	135
15.2.5	AVA_VAN.3 Focused vulnerability analysis	136
15.2.6	AVA_VAN.4 Methodical vulnerability analysis	137
15.2.7	AVA_VAN.5 Advanced methodical vulnerability analysis	138
16	Class ACO: Composition	139
16.1	Composition rationale (ACO_COR)	141
16.1.1	Objectives	141
16.1.2	Component levelling	141
16.1.3	ACO_COR.1 Composition rationale	142
16.2	Development evidence (ACO_DEV)	142
16.2.1	Objectives	142
16.2.2	Component levelling	142
16.2.3	Application notes	142
16.2.4	ACO_DEV.1 Functional Description	143

16.2.5	ACO_DEV.2 Basic evidence of design	143
16.2.6	ACO_DEV.3 Detailed evidence of design	144
16.3	Reliance of dependent component (ACO_REL)	145
16.3.1	Objectives	145
16.3.2	Component levelling	146
16.3.3	Application notes	146
16.3.4	ACO_REL.1 Basic reliance information	146
16.3.5	ACO_REL.2 Reliance information	147
16.4	Composed TOE testing (ACO_CTT)	147
16.4.1	Objectives	147
16.4.2	Component levelling	147
16.4.3	Application notes	147
16.4.4	ACO_CTT.1 Interface testing	148
16.4.5	ACO_CTT.2 Rigorous interface testing	149
16.5	Composition vulnerability analysis (ACO_VUL)	150
16.5.1	Objectives	150
16.5.2	Component levelling	150
16.5.3	Application notes	151
16.5.4	ACO_VUL.1 Composition vulnerability review	151
16.5.5	ACO_VUL.2 Composition vulnerability analysis	152
16.5.6	ACO_VUL.3 Enhanced-Basic Composition vulnerability analysis	152
Annex A (informative) Development (ADV)		154
A.1	ADV_ARC: Supplementary material on security architectures	154
A.1.1	Security architecture properties	154
A.1.2	Security architecture descriptions	155
A.2	ADV_FSP: Supplementary material on TSFIs	157
A.2.1	Determining the TSFI	157
A.2.2	Example: A complex DBMS	159
A.2.3	Example Functional Specification	160
A.3	ADV_INT: Supplementary material on TSF internals	162
A.3.1	Structure of procedural software	162
A.3.2	Complexity of procedural software	164
A.4	ADV_TDS: Subsystems and Modules	165
A.4.1	Subsystems	165
A.4.2	Modules	166
A.4.3	Levelling Approach	168
A.5	Supplementary material on formal methods	170
Annex B (informative) Composition (ACO)		172
B.1	Necessity for composed TOE evaluations	172
B.2	Performing Security Target evaluation for a composed TOE	173
B.3	Interactions between composed IT entities	174
Annex C (informative) Cross reference of assurance component dependencies		179
Annex D (informative) Cross reference of PPs and assurance components		183
Annex E (informative) Cross reference of EALs and assurance components		184
Annex F (informative) Cross reference of CAPs and assurance components		185