

ISO/IEC 15408-3:2008-08 (E)

Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components

Contents		Page
Foreword		ix
Introduction		xi
1	Scope	1
2	Normative references	1
3	Terms and definitions, symbols and abbreviated terms	1
4	Overview	1
5	Assurance paradigm	2
5.2	Assurance approach	2
5.2.1	Significance of vulnerabilities	2
5.2.2	Cause of vulnerabilities	3
5.2.4	Assurance through evaluation	3
6	Security assurance components	4
6.1	Security assurance classes, families and components structure	4
6.1.1	Assurance class structure	4
6.1.2	Assurance family structure	5
6.1.3	Assurance component structure	6
6.1.4	Assurance elements	8
6.1.5	Component taxonomy	8
6.2	EAL structure	9
6.2.1	EAL name	9
6.2.2	Objectives	9
6.2.3	Application notes	9
6.2.4	Assurance components	10
6.2.5	Relationship between assurances and assurance levels	10
6.3	CAP structure	11
6.3.1	CAP name	11
6.3.2	Objectives	11
6.3.3	Application notes	11
6.3.4	Assurance components	12
6.3.5	Relationship between assurances and assurance levels	13
7	Evaluation assurance levels	13
7.1	Evaluation assurance level (EAL) overview	14
7.2	Evaluation assurance level details	15
7.3	Evaluation assurance level 1 (EAL1) - functionally tested	15
7.3.1	Objectives	15
7.3.2	Assurance components	16
7.4	Evaluation assurance level 2 (EAL2) - structurally tested	16
7.4.1	Objectives	16
7.4.2	Assurance components	16
7.5	Evaluation assurance level 3 (EAL3) - methodically tested and checked	17
7.5.1	Objectives	17
7.5.2	Assurance components	17
7.6	Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed	18

7.6.1	Objectives	18
7.6.2	Assurance components	18
7.7	Evaluation assurance level 5 (EAL5) - semiformally designed and tested	19
7.7.1	Objectives	19
7.7.2	Assurance components	19
7.8	Evaluation assurance level 6 (EAL6) - semiformally verified design and tested	20
7.8.1	Objectives	20
7.8.2	Assurance components	20
7.9	Evaluation assurance level 7 (EAL7) - formally verified design and tested	21
7.9.1	Objectives	21
7.9.2	Assurance components	22
8	Composed assurance packages	23
8.1	Composed assurance package (CAP) overview	23
8.2	Composed assurance package details	24
8.3	Composition assurance level A (CAP-A) - Structurally composed	24
8.3.1	Objectives	24
8.3.2	Assurance components	24
8.4	Composition assurance level B (CAP-B) - Methodically composed	25
8.4.1	Objectives	25
8.4.2	Assurance components	25
8.5	Composition assurance level C (CAP-C) - Methodically composed, tested and reviewed	26
8.5.1	Objectives	26
8.5.2	Assurance components	26
9	Class APE: Protection Profile evaluation	27
9.1	PP introduction (APE_INT)	28
9.1.1	Objectives	28
9.1.2	APE_INT.1 PP introduction	28
9.2	Conformance claims (APE_CCL)	29
9.2.1	Objectives	29
9.2.2	APE_CCL.1 Conformance claims	29
9.3	Security problem definition (APE_SPD)	31
9.3.1	Objectives	31
9.3.2	APE_SPD.1 Security problem definition	31
9.4	Security objectives (APE_OBJ)	31
9.4.1	Objectives	31
9.4.2	Component levelling	32
9.4.3	APE_OBJ.1 Security objectives for the operational environment	32
9.4.4	APE_OBJ.2 Security objectives	32
9.5	Extended components definition (APE_ECD)	33
9.5.1	Objectives	33
9.5.2	APE_ECD.1 Extended components definition	33
9.6	Security requirements (APE_REQ)	34
9.6.1	Objectives	34
9.6.2	Component levelling	34
9.6.3	APE_REQ.1 Stated security requirements	34
9.6.4	APE_REQ.2 Derived security requirements	35
10	Class ASE: Security Target evaluation	36
10.1	ST introduction (ASE_INT)	37
10.1.1	Objectives	37
10.1.2	ASE_INT.1 ST introduction	37
10.2	Conformance claims (ASE_CCL)	38
10.2.1	Objectives	38
10.2.2	ASE_CCL.1 Conformance claims	38
10.3	Security problem definition (ASE_SPD)	40
10.3.1	Objectives	40
10.3.2	ASE_SPD.1 Security problem definition	40
10.4	Security objectives (ASE_OBJ)	41
10.4.1	Objectives	41
10.4.2	Component levelling	41

10.4.3	ASE_OBJ.1 Security objectives for the operational environment	41
10.4.4	ASE_OBJ.2 Security objectives	41
10.5	Extended components definition (ASE_ECD)	42
10.5.1	Objectives	42
10.5.2	ASE_ECD.1 Extended components definition	42
10.6	Security requirements (ASE_REQ)	43
10.6.1	Objectives	43
10.6.2	Component levelling	43
10.6.3	ASE_REQ.1 Stated security requirements	44
10.6.4	ASE_REQ.2 Derived security requirements	44
10.7	TOE summary specification (ASE_TSS)	46
10.7.1	Objectives	46
10.7.2	Component levelling	46
10.7.3	ASE_TSS.1 TOE summary specification	46
10.7.4	ASE_TSS.2 TOE summary specification with architectural design summary	47
11	Class ADV: Development	48
11.1	Security Architecture (ADV_ARC)	52
11.1.1	Objectives	52
11.1.2	Component levelling	52
11.1.3	Application notes	52
11.1.4	ADV_ARC.1 Security architecture description	53
11.2	Functional specification (ADV_FSP)	54
11.2.1	Objectives	54
11.2.2	Component levelling	54
11.2.3	Application notes	54
11.2.4	ADV_FSP.1 Basic functional specification	56
11.2.5	ADV_FSP.2 Security-enforcing functional specification	57
11.2.6	ADV_FSP.3 Functional specification with complete summary	58
11.2.7	ADV_FSP.4 Complete functional specification	59
11.2.8	ADV_FSP.5 Complete semi-formal functional specification with additional error information	60
11.2.9	ADV_FSP.6 Complete semi-formal functional specification with additional formal specification	61
11.3	Implementation representation (ADV_IMP)	63
11.3.1	Objectives	63
11.3.2	Component levelling	63
11.3.3	Application notes	63
11.3.4	ADV_IMP.1 Implementation representation of the TSF	64
11.3.5	ADV_IMP.2 Complete mapping of the implementation representation of the TSF	64
11.4	TSF internals (ADV_INT)	65
11.4.1	Objectives	65
11.4.2	Component levelling	65
11.4.3	Application notes	65
11.4.4	ADV_INT.1 Well-structured subset of TSF internals	66
11.4.5	ADV_INT.2 Well-structured internals	67
11.4.6	ADV_INT.3 Minimally complex internals	68
11.5	Security policy modelling (ADV_SPM)	69
11.5.1	Objectives	69
11.5.2	Component levelling	69
11.5.3	Application notes	69
11.5.4	ADV_SPM.1 Formal TOE security policy model	70
11.6	TOE design (ADV_TDS)	71
11.6.1	Objectives	71
11.6.2	Component levelling	71
11.6.3	Application notes	71
11.6.4	ADV_TDS.1 Basic design	72
11.6.5	ADV_TDS.2 Architectural design	73
11.6.6	ADV_TDS.3 Basic modular design	74
11.6.7	ADV_TDS.4 Semiformal modular design	76
11.6.8	ADV_TDS.5 Complete semiformal modular design	77

11.6.9	ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation	78
12	Class AGD: Guidance documents	80
12.1	Operational user guidance (AGD_OPE)	80
12.1.1	Objectives	80
12.1.2	Component levelling	81
12.1.3	Application notes	81
12.1.4	AGD_OPE.1 Operational user guidance	81
12.2	Preparative procedures (AGD_PRE)	82
12.2.1	Objectives	82
12.2.2	Component levelling	82
12.2.3	Application notes	82
12.2.4	AGD_PRE.1 Preparative procedures	83
13	Class ALC: Life-cycle support	83
13.1	CM capabilities (ALC_CMC)	84
13.1.1	Objectives	84
13.1.2	Component levelling	85
13.1.3	Application notes	85
13.1.4	ALC_CMC.1 Labelling of the TOE	85
13.1.5	ALC_CMC.2 Use of a CM system	86
13.1.6	ALC_CMC.3 Authorisation controls	87
13.1.7	ALC_CMC.4 Production support, acceptance procedures and automation	88
13.1.8	ALC_CMC.5 Advanced support	90
13.2	CM scope (ALC_CMS)	92
13.2.1	Objectives	92
13.2.2	Component levelling	93
13.2.3	Application notes	93
13.2.4	ALC_CMS.1 TOE CM coverage	93
13.2.5	ALC_CMS.2 Parts of the TOE CM coverage	93
13.2.6	ALC_CMS.3 Implementation representation CM coverage	94
13.2.7	ALC_CMS.4 Problem tracking CM coverage	95
13.2.8	ALC_CMS.5 Development tools CM coverage	96
13.3	Delivery (ALC_DEL)	97
13.3.1	Objectives	97
13.3.2	Component levelling	97
13.3.3	Application notes	97
13.3.4	ALC_DEL.1 Delivery procedures	98
13.4	Development security (ALC_DVS)	98
13.4.1	Objectives	98
13.4.2	Component levelling	98
13.4.3	Application notes	98
13.4.4	ALC_DVS.1 Identification of security measures	99
13.4.5	ALC_DVS.2 Sufficiency of security measures	99
13.5	Flaw remediation (ALC_FLR)	100
13.5.1	Objectives	100
13.5.2	Component levelling	100
13.5.3	Application notes	100
13.5.4	ALC_FLR.1 Basic flaw remediation	100
13.5.5	ALC_FLR.2 Flaw reporting procedures	101
13.5.6	ALC_FLR.3 Systematic flaw remediation	102
13.6	Life-cycle definition (ALC_LCD)	104
13.6.1	Objectives	104
13.6.2	Component levelling	104
13.6.3	Application notes	104
13.6.4	ALC_LCD.1 Developer defined life-cycle model	105
13.6.5	ALC_LCD.2 Measurable life-cycle model	106
13.7	Tools and techniques (ALC_TAT)	106
13.7.1	Objectives	106
13.7.2	Component levelling	107
13.7.3	Application notes	107

13.7.4	ALC_TAT.1 Well-defined development tools	107
13.7.5	ALC_TAT.2 Compliance with implementation standards	108
13.7.6	ALC_TAT.3 Compliance with implementation standards - all parts	108
14	Class ATE: Tests	109
14.1	Coverage (ATE_COV)	110
14.1.1	Objectives	110
14.1.2	Component levelling	110
14.1.3	Application notes	110
14.1.4	ATE_COV.1 Evidence of coverage	110
14.1.5	ATE_COV.2 Analysis of coverage	111
14.1.6	ATE_COV.3 Rigorous analysis of coverage	112
14.2	Depth (ATE_DPT)	112
14.2.1	Objectives	112
14.2.2	Component levelling	113
14.2.3	Application notes	113
14.2.4	ATE_DPT.1 Testing: basic design	113
14.2.5	ATE_DPT.2 Testing: security enforcing modules	114
14.2.6	ATE_DPT.3 Testing: modular design	114
14.2.7	ATE_DPT.4 Testing: implementation representation	115
14.3	Functional tests (ATE_FUN)	116
14.3.1	Objectives	116
14.3.2	Component levelling	116
14.3.3	Application notes	116
14.3.4	ATE_FUN.1 Functional testing	117
14.3.5	ATE_FUN.2 Ordered functional testing	117
14.4	Independent testing (ATE_IND)	118
14.4.1	Objectives	118
14.4.2	Component levelling	118
14.4.3	Application notes	119
14.4.4	ATE_IND.1 Independent testing - conformance	119
14.4.5	ATE_IND.2 Independent testing - sample	120
14.4.6	ATE_IND.3 Independent testing - complete	121
15	Class AVA: Vulnerability assessment	122
15.1	Application notes	122
15.2	Vulnerability analysis (AVA_VAN)	123
15.2.1	Objectives	123
15.2.2	Component levelling	123
15.2.3	AVA_VAN.1 Vulnerability survey	123
15.2.4	AVA_VAN.2 Vulnerability analysis	124
15.2.5	AVA_VAN.3 Focused vulnerability analysis	125
15.2.6	AVA_VAN.4 Methodical vulnerability analysis	126
15.2.7	AVA_VAN.5 Advanced methodical vulnerability analysis	127
16	Class ACO: Composition	128
16.1	Composition rationale (ACO_COR)	130
16.1.1	Objectives	130
16.1.2	Component levelling	130
16.1.3	ACO_COR.1 Composition rationale	131
16.2	Development evidence (ACO_DEV)	131
16.2.1	Objectives	131
16.2.2	Component levelling	131
16.2.3	Application notes	131
16.2.4	ACO_DEV.1 Functional Description	132
16.2.5	ACO_DEV.2 Basic evidence of design	132
16.2.6	ACO_DEV.3 Detailed evidence of design	133
16.3	Reliance of dependent component (ACO_REL)	134
16.3.1	Objectives	134
16.3.2	Component levelling	135
16.3.3	Application notes	135
16.3.4	ACO_REL.1 Basic reliance information	135

16.3.5	ACO_REL.2 Reliance information	136
16.4	Composed TOE testing (ACO_CTT)	136
16.4.1	Objectives	136
16.4.2	Component levelling	136
16.4.3	Application notes	136
16.4.4	ACO_CTT.1 Interface testing	137
16.4.5	ACO_CTT.2 Rigorous interface testing	138
16.5	Composition vulnerability analysis (ACO_VUL)	139
16.5.1	Objectives	139
16.5.2	Component levelling	139
16.5.3	Application notes	140
16.5.4	ACO_VUL.1 Composition vulnerability review	140
16.5.5	ACO_VUL.2 Composition vulnerability analysis	141
16.5.6	ACO_VUL.3 Enhanced-Basic Composition vulnerability analysis	141
Annex A (informative) Development (ADV)		143
A.1	ADV_ARC: Supplementary material on security architectures	143
A.1.1	Security architecture properties	143
A.1.2	Security architecture descriptions	144
A.2	ADV_FSP: Supplementary material on TSFIs	146
A.2.1	Determining the TSFI	146
A.2.2	Example: A complex DBMS	148
A.2.3	Example Functional Specification	149
A.3	ADV_INT: Supplementary material on TSF internals	151
A.3.1	Structure of procedural software	151
A.3.2	Complexity of procedural software	153
A.4	ADV_TDS: Subsystems and Modules	154
A.4.1	Subsystems	154
A.4.2	Modules	155
A.4.3	Levelling Approach	157
A.5	Supplementary material on formal methods	159
Annex B (informative) Composition (ACO)		161
B.1	Necessity for composed TOE evaluations	161
B.2	Performing Security Target evaluation for a composed TOE	162
B.3	Interactions between composed IT entities	163
Annex C (informative) Cross reference of assurance component dependencies		168
Annex D (informative) Cross reference of PPs and assurance components		172
Annex E (informative) Cross reference of EALs and assurance components		173
Annex F (informative) Cross reference of CAPs and assurance components		174