ISO/IEC 15408-3:2026-05 (E)

Information security, cybersecurity and privacy protection - Evaluation criteria for IT security - Part 3: Security assurance components

Contents

Page

Foreword ..... **x**

Introduction ..... **xi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Overview **5**

5 Assurance paradigm **5**
5.1 General 5
5.2 CC approach 5
5.3 Assurance approach 5
5.3.1 General 5
5.3.2 Significance of vulnerabilities 5
5.3.3 Cause of vulnerabilities 6
5.3.4 CC assurance 6
5.3.5 Assurance through evaluation 6
5.4 CC evaluation assurance scale 7

6 Security assurance components **7**
6.1 General 7
6.2 Assurance class structure 7
6.2.1 General 7
6.2.2 Class name 8
6.2.3 Class introduction 8
6.2.4 Class application notes 8
6.2.5 Assurance families 8
6.3 Assurance family structure 8
6.3.1 General 8
6.3.2 Family name 8
6.3.3 Family objectives 8
6.3.4 Component levelling 9
6.3.5 Family application notes 9
6.3.6 Assurance components 9
6.4 Assurance component structure 9
6.4.1 General 9
6.4.2 Component name 9
6.4.3 Component objectives 10
6.4.4 Component application notes 10
6.4.5 Component dependencies 10
6.4.6 Assurance elements 10
6.5 Assurance elements 11
6.6 Component taxonomy 11

7 Class APE Protection Profile (PP) evaluation **11**
7.1 General 11
7.2 PP introduction (APE_INT) 12
7.2.1 Objectives 12
7.2.2 PP introduction (APE_INT.1) 13
7.3 Conformance claims (APE_CCL) 13
7.3.1 Objectives 13
7.3.2 Conformance claims (APE_CCL.1) 13

7.4 Security problem definition (APE_SPD) 15
7.4.1 Objectives 15
7.4.2 Security problem definition (APE_SPD.1) 15
7.5 Security objectives (APE_OBJ) 15
7.5.1 Objectives 15
7.5.2 Component levelling 15
7.5.3 Security objectives for the operational environment (APE_OBJ.1) 15
7.5.4 Security objectives (APE_OBJ.2) 16
7.6 Extended components definition (APE_ECD) 17
7.6.1 Objectives 17
7.6.2 Extended components definition (APE_ECD.1) 17
7.7 Security requirements (APE_REQ) 18
7.7.1 Objectives 18
7.7.2 Component levelling 18
7.7.3 Direct rationale security requirements (APE_REQ.1) 18
7.7.4 Derived security requirements (APE_REQ.2) 19

8 Class ACE Protection Profile Configuration evaluation 20
8.1 General 20
8.2 PP-Module introduction (ACE_INT) 22
8.2.1 Objectives 22
8.2.2 PP-Module introduction (ACE_INT.1) 22
8.3 PP-Module conformance claims (ACE_CCL) 22
8.3.1 Objectives 22
8.3.2 PP-Module conformance claims (ACE_CCL.1) 23
8.4 PP-Module security problem definition (ACE_SPD) 24
8.4.1 Objectives 24
8.4.2 PP-Module security problem definition (ACE_SPD.1) 24
8.5 PP-Module security objectives (ACE_OBJ) 24
8.5.1 Objectives 24
8.5.2 Component levelling 24
8.5.3 PP-Module security objectives for the operational environment (ACE_OBJ.1) 24
8.5.4 PP-Module security objectives (ACE_OBJ.2) 25
8.6 PP-Module extended components definition (ACE_ECD) 26
8.6.1 Objectives 26
8.6.2 PP-Module extended components definition (ACE_ECD.1) 26
8.7 PP-Module security requirements (ACE_REQ) 27
8.7.1 Objectives 27
8.7.2 Component levelling 27
8.7.3 PP-Module direct rationale security requirements (ACE_REQ.1) 27
8.7.4 PP-Module derived security requirements (ACE_REQ.2) 28
8.8 PP-Module consistency (ACE_MCO) 29
8.8.1 Objectives 29
8.8.2 PP-Module consistency (ACE_MCO.1) 29
8.9 PP-Configuration consistency (ACE_CCO) 30
8.9.1 Objectives 30
8.9.2 PP-Configuration consistency (ACE_CCO.1) 30

9 Class ASE Security Target (ST) evaluation 32
9.1 General 32
9.2 ST introduction (ASE_INT) 34
9.2.1 Objectives 34
9.2.2 ST introduction (ASE_INT.1) 34
9.3 Conformance claims (ASE_CCL) 34
9.3.1 Objectives 34
9.3.2 Conformance claims (ASE_CCL.1) 35
9.4 Security problem definition (ASE_SPD) 36
9.4.1 Objectives 36
9.4.2 Security problem definition (ASE_SPD.1) 36
9.5 Security objectives (ASE_OBJ) 36
9.5.1 Objectives 36
9.5.2 Component levelling 36
9.5.3 Security objectives for the operational environment (ASE_OBJ.1) 36
9.5.4 Security objectives (ASE_OBJ.2) 37

9.6 Extended components definition (ASE_ECD) 38
9.6.1 Objectives 38
9.6.2 Extended components definition (ASE_ECD.1) 38
9.7 Security requirements (ASE_REQ) 39
9.7.1 Objectives 39
9.7.2 Component levelling 39
9.7.3 Direct rationale security requirements (ASE_REQ.1) 39
9.7.4 Derived security requirements (ASE_REQ.2) 40
9.8 TOE summary specification (ASE_TSS) 41
9.8.1 Objectives 41
9.8.2 Component levelling 41
9.8.3 TOE summary specification (ASE_TSS.1) 41
9.8.4 TOE summary specification with architectural design summary (ASE_TSS.2) 42
9.9 Consistency of composite product Security Target (ASE_COMP) 42
9.9.1 Objectives 42
9.9.2 Component levelling 43
9.9.3 Application notes 43
9.9.4 Consistency of Security Target (ST) (ASE_COMP.1) 44

10 Class ADV Development 44
10.1 General 44
10.2 Security architecture (ADV_ARC) 50
10.2.1 Objectives 50
10.2.2 Component levelling 50
10.2.3 Application notes 50
10.2.4 Security architecture description (ADV_ARC.1) 51
10.3 Functional specification (ADV_FSP) 52
10.3.1 Objectives 52
10.3.2 Component levelling 52
10.3.3 Application notes 52
10.3.4 Basic functional specification (ADV_FSP.1) 55
10.3.5 Security-enforcing functional specification (ADV_FSP.2) 55
10.3.6 Functional specification with complete summary (ADV_FSP.3) 56
10.3.7 Complete functional specification (ADV_FSP.4) 57
10.3.8 Complete semi-formal functional specification with additional error information (ADV_FSP.5) 57
10.3.9 Complete semi-formal functional specification with additional formal specification (ADV_FSP.6) 58
10.4 Implementation representation (ADV_IMP) 59
10.4.1 Objectives 59
10.4.2 Component levelling 59
10.4.3 Application notes 59
10.4.4 Implementation representation of the TSF (ADV_IMP.1) 60
10.4.5 Complete mapping of the implementation representation of the TSF (ADV_IMP.2) 61
10.5 TSF internals (ADV_INT) 62
10.5.1 Objectives 62
10.5.2 Component levelling 62
10.5.3 Application notes 62
10.5.4 Well-structured subset of TSF internals (ADV_INT.1) 62
10.5.5 Well-structured internals (ADV_INT.2) 63
10.5.6 Minimally complex internals (ADV_INT.3) 64
10.6 Formal TSF model (ADV_SPM) 65
10.6.1 Objectives 65
10.6.2 Component levelling 65
10.6.3 Application notes 65
10.6.4 Formal TSF model (ADV_SPM.1) 66
10.7 TOE design (ADV_TDS) 67
10.7.1 Objectives 67
10.7.2 Component levelling 67

10.7.3 Application notes 67
10.7.4 Basic design (ADV_TDS.1) 68
10.7.5 Architectural design (ADV_TDS.2) 69
10.7.6 Basic modular design (ADV_TDS.3) 70
10.7.7 Semi-Formal modular design (ADV_TDS.4) 71
10.7.8 Complete semi-formal modular design (ADV_TDS.5) 71
10.7.9 Complete semi-formal modular design with formal high-level design presentation (ADV_TDS.6) 72
10.8 Composite design compliance (ADV_COMP) 73
10.8.1 Objectives 73
10.8.2 Component levelling 73
10.8.3 Application notes 73
10.8.4 Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority (ADV_COMP.1) 74

11 Class AGD guidance documents 75
11.1 General 75
11.2 Operational user guidance (AGD_OPE) 75
11.2.1 Objectives 75
11.2.2 Component levelling 76
11.2.3 Application notes 76
11.2.4 Operational user guidance (AGD_OPE.1) 76
11.3 Preparative procedures (AGD_PRE) 77
11.3.1 Objectives 77
11.3.2 Component levelling 77
11.3.3 Application notes 77
11.3.4 Preparative procedures (AGD_PRE.1) 78

12 Class ALC life cycle support 78
12.1 General 78
12.2 CM capabilities (ALC_CMC) 80
12.2.1 Objectives 80
12.2.2 Component levelling 81
12.2.3 Application notes 81
12.2.4 Labelling of the TOE (ALC_CMC.1) 81
12.2.5 Use of the CM system (ALC_CMC.2) 82
12.2.6 Authorization controls (ALC_CMC.3) 83
12.2.7 Production support, acceptance procedures and automation (ALC_CMC.4) 84
12.2.8 Advanced support (ALC_CMC.5) 85
12.3 CM scope (ALC_CMS) 87
12.3.1 Objectives 87
12.3.2 Component levelling 87
12.3.3 Application notes 87
12.3.4 TOE CM coverage (ALC_CMS.1) 87
12.3.5 Parts of the TOE CM coverage (ALC_CMS.2) 88
12.3.6 Implementation representation CM coverage (ALC_CMS.3) 89
12.3.7 Problem tracking CM coverage (ALC_CMS.4) 89
12.3.8 Development tools CM coverage (ALC_CMS.5) 90
12.4 Delivery (ALC_DEL) 91
12.4.1 Objectives 91
12.4.2 Component levelling 91
12.4.3 Application notes 91
12.4.4 Delivery procedures (ALC_DEL.1) 92
12.5 Developer environment security (ALC_DVS) 92
12.5.1 Objectives 92
12.5.2 Component levelling 92
12.5.3 Application notes 93
12.5.4 Identification of security controls (ALC_DVS.1) 93
12.5.5 Sufficiency of security controls (ALC_DVS.2) 93

12.6 Flaw remediation (ALC_FLR) ... 94
12.6.1 Objectives ... 94
12.6.2 Component levelling ... 94
12.6.3 Application notes ... 94
12.6.4 Basic flaw remediation (ALC_FLR.1) ... 94
12.6.5 Flaw reporting procedures (ALC_FLR.2) ... 95
12.6.6 Systematic flaw remediation (ALC_FLR.3) ... 96
12.7 Development life cycle definition (ALC_LCD) ... 97
12.7.1 Objectives ... 97
12.7.2 Component levelling ... 97
12.7.3 Application notes ... 97
12.7.4 Developer defined life cycle processes (ALC_LCD.1) ... 98
12.7.5 Measurable life cycle model (ALC_LCD.2) ... 98
12.8 TOE development artefacts (ALC_TDA) ... 99
12.8.1 Objectives ... 99
12.8.2 Component levelling ... 99
12.8.3 Application notes ... 99
12.8.4 Uniquely identifying implementation representation (ALC_TDA.1) ... 100
12.8.5 Matching CMS scope of implementation representation (ALC_TDA.2) ... 101
12.8.6 Regenerate TOE with well-defined development tools (ALC_TDA.3) ... 103
12.9 Tools and techniques (ALC_TAT) ... 105
12.9.1 Objectives ... 105
12.9.2 Component levelling ... 105
12.9.3 Application notes ... 105
12.9.4 Well-defined development tools (ALC_TAT.1) ... 106
12.9.5 Compliance with implementation standards (ALC_TAT.2) ... 106
12.9.6 Compliance with implementation standards - all parts (ALC_TAT.3) ... 107
12.10 Integration of composition parts and consistency check of delivery procedures (ALC_COMP) ... 108
12.10.1 Objectives ... 108
12.10.2 Component levelling ... 108
12.10.3 Application notes ... 108
12.10.4 Integration of the dependent component into the related base component and Consistency check for delivery and acceptance procedures (ALC_COMP.1) ... 108

13 Class ATE Tests ... 109
13.1 General ... 109
13.2 Coverage (ATE_COV) ... 110
13.2.1 Objectives ... 110
13.2.2 Component levelling ... 111
13.2.3 Evidence of coverage (ATE_COV.1) ... 111
13.2.4 Analysis of coverage (ATE_COV.2) ... 111
13.2.5 Rigorous analysis of coverage (ATE_COV.3) ... 112
13.3 Depth (ATE_DPT) ... 113
13.3.1 Objectives ... 113
13.3.2 Component levelling ... 113
13.3.3 Application notes ... 113
13.3.4 Testing: basic design (ATE_DPT.1) ... 113
13.3.5 Testing: security enforcing modules (ATE_DPT.2) ... 114
13.3.6 Testing: modular design (ATE_DPT.3) ... 115
13.3.7 Testing: implementation representation (ATE_DPT.4) ... 116
13.4 Functional tests (ATE_FUN) ... 116
13.4.1 Objectives ... 116
13.4.2 Component levelling ... 117
13.4.3 Application notes ... 117
13.4.4 Functional testing (ATE_FUN.1) ... 117
13.4.5 Ordered functional testing (ATE_FUN.2) ... 118
13.5 Independent testing (ATE_IND) ... 118
13.5.1 Objectives ... 118

13.5.2 Component levelling 119
13.5.3 Application notes 119
13.5.4 Independent testing - conformance (ATE_IND.1) 119
13.5.5 Independent testing - sample (ATE_IND.2) 120
13.5.6 Independent testing - complete (ATE_IND.3) 121
13.6 Composite functional testing (ATE_COMP) 122
13.6.1 Objectives 122
13.6.2 Component levelling 122
13.6.3 Application notes 122
13.6.4 Composite product functional testing (ATE_COMP.1) 123
14 Class AVA Vulnerability assessment 123
14.1 General 123
14.2 Application notes 124
14.3 Vulnerability analysis (AVA_VAN) 124
14.3.1 Objectives 124
14.3.2 Component levelling 125
14.3.3 Vulnerability survey (AVA_VAN.1) 125
14.3.4 Vulnerability analysis (AVA_VAN.2) 126
14.3.5 Focused vulnerability analysis (AVA_VAN.3) 127
14.3.6 Methodical vulnerability analysis (AVA_VAN.4) 128
14.3.7 Advanced methodical vulnerability analysis (AVA_VAN.5) 129
14.4 Composite vulnerability assessment (AVA_COMP) 130
14.4.1 Objectives 130
14.4.2 Component levelling 130
14.4.3 Application notes 130
14.4.4 Composite product vulnerability assessment (AVA_COMP.1) 131
15 Class ACO Composition 131
15.1 General 131
15.2 Composition rationale (ACO_COR) 135
15.2.1 Objectives 135
15.2.2 Component levelling 135
15.2.3 Composition rationale (ACO_COR.1) 136
15.3 Development evidence (ACO_DEV) 136
15.3.1 Objectives 136
15.3.2 Component levelling 136
15.3.3 Application notes 136
15.3.4 Functional description (ACO_DEV.1) 137
15.3.5 Basic evidence of design (ACO_DEV.2) 137
15.3.6 Detailed evidence of design (ACO_DEV.3) 138
15.4 Reliance of dependent component (ACO_REL) 139
15.4.1 Objectives 139
15.4.2 Component levelling 139
15.4.3 Application notes 139
15.4.4 Basic reliance information (ACO_REL.1) 140
15.4.5 Reliance information (ACO_REL.2) 140
15.5 Composed TOE testing (ACO_CTT) 141
15.5.1 Objectives 141
15.5.2 Component levelling 141
15.5.3 Application notes 141
15.5.4 Interface testing (ACO_CTT.1) 141
15.5.5 Rigorous interface testing (ACO_CTT.2) 142
15.6 Composition vulnerability analysis (ACO_VUL) 143
15.6.1 Objectives 143
15.6.2 Component levelling 143
15.6.3 Application notes 143
15.6.4 Composition vulnerability review (ACO_VUL.1) 144
15.6.5 Composition vulnerability analysis (ACO_VUL.2) 144
15.6.6 Enhanced-Basic composition vulnerability analysis (ACO_VUL.3) 145

Annex A (informative) **Development (ADV)** **146**
Annex B (informative) **Composition (ACO)** **167**
Bibliography **176**