

---

---

**Information security, cybersecurity and privacy protection — Evaluation criteria for IT security —**

**Part 3:  
Security assurance components**

*Sécurité de l'information, cybersécurité et protection de la vie privée — Critères d'évaluation pour la sécurité des technologies de l'information —*

*Partie 3: Composants d'assurance de sécurité*





**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office  
CP 401 • Ch. de Blandonnet 8  
CH-1214 Vernier, Geneva  
Phone: +41 22 749 01 11  
Email: [copyright@iso.org](mailto:copyright@iso.org)  
Website: [www.iso.org](http://www.iso.org)

Published in Switzerland

# Contents

	Page
Foreword.....	x
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 Overview.....</b>	<b>5</b>
<b>5 Assurance paradigm.....</b>	<b>6</b>
5.1 General.....	6
5.2 ISO/IEC 15408 series approach.....	6
5.3 Assurance approach.....	6
5.3.1 General.....	6
5.3.2 Significance of vulnerabilities.....	6
5.3.3 Cause of vulnerabilities.....	7
5.3.4 ISO/IEC 15408 series assurance.....	7
5.3.5 Assurance through evaluation.....	7
5.4 ISO/IEC 15408 series evaluation assurance scale.....	8
<b>6 Security assurance components.....</b>	<b>8</b>
6.1 General.....	8
6.2 Assurance class structure.....	8
6.2.1 General.....	8
6.2.2 Class name.....	8
6.2.3 Class introduction.....	8
6.2.4 Assurance families.....	9
6.3 Assurance family structure.....	9
6.3.1 Family name.....	9
6.3.2 Objectives.....	9
6.3.3 Component levelling.....	10
6.3.4 Application notes.....	10
6.3.5 Assurance components.....	10
6.4 Assurance component structure.....	10
6.4.1 General.....	10
6.4.2 Component identification.....	11
6.4.3 Objectives.....	11
6.4.4 Application notes.....	11
6.4.5 Dependencies.....	11
6.4.6 Assurance elements.....	11
6.5 Assurance elements.....	12
6.6 Component taxonomy.....	12
<b>7 Class APE: Protection Profile (PP) evaluation.....</b>	<b>12</b>
7.1 General.....	12
7.2 PP introduction (APE_INT).....	13
7.2.1 Objectives.....	13
7.2.2 APE_INT.1 PP introduction.....	13
7.3 Conformance claims (APE_CCL).....	14
7.3.1 Objectives.....	14
7.3.2 APE_CCL.1 Conformance claims.....	14
7.4 Security problem definition (APE_SPD).....	16
7.4.1 Objectives.....	16
7.4.2 APE_SPD.1 Security problem definition.....	16
7.5 Security objectives (APE_OBJ).....	16
7.5.1 Objectives.....	16
7.5.2 Component levelling.....	17

7.5.3	APE_OBJ.1 Security objectives for the operational environment.....	17
7.5.4	APE_OBJ.2 Security objectives.....	17
7.6	Extended components definition (APE_ECD).....	18
7.6.1	Objectives.....	18
7.6.2	APE_ECD.1 Extended components definition.....	18
7.7	Security requirements (APE_REQ).....	19
7.7.1	Objectives.....	19
7.7.2	Component levelling.....	19
7.7.3	APE_REQ.1 Direct rationale PP-Module security requirements.....	19
7.7.4	APE_REQ.2 Derived security requirements.....	20
<b>8</b>	<b>Class ACE: Protection Profile Configuration evaluation.....</b>	<b>22</b>
8.1	General.....	22
8.2	PP-Module introduction (ACE_INT).....	22
8.2.1	Objectives.....	22
8.2.2	ACE_INT.1 PP-Module introduction.....	22
8.3	PP-Module conformance claims (ACE_CCL).....	23
8.3.1	Objectives.....	23
8.3.2	ACE_CCL.1 PP-Module conformance claims.....	23
8.4	PP-Module security problem definition (ACE_SPD).....	25
8.4.1	Objectives.....	25
8.4.2	ACE_SPD.1 PP-Module security problem definition.....	25
8.5	PP-Module security objectives (ACE_OBJ).....	26
8.5.1	Objectives.....	26
8.5.2	Component levelling.....	26
8.5.3	ACE_OBJ.1 PP-Module security objectives for the operational environment.....	26
8.5.4	ACE_OBJ.2 PP-Module security objectives.....	27
8.6	PP-Module extended components definition (ACE_ECD).....	27
8.6.1	Objectives.....	27
8.6.2	ACE_ECD.1 PP-Module extended components definition.....	28
8.7	PP-Module security requirements (ACE_REQ).....	28
8.7.1	Objectives.....	28
8.7.2	Component levelling.....	29
8.7.3	ACE_REQ.1 PP-Module stated security requirements.....	29
8.7.4	ACE_REQ.2 PP-Module derived security requirements.....	30
8.8	PP-Module consistency (ACE_MCO).....	31
8.8.1	Objectives.....	31
8.8.2	ACE_MCO.1 PP-Module consistency.....	31
8.9	PP-Configuration consistency (ACE_CCO).....	32
8.9.1	Objectives.....	32
8.9.2	ACE_CCO.1 PP-Configuration consistency.....	32
<b>9</b>	<b>Class ASE: Security Target (ST) evaluation.....</b>	<b>36</b>
9.1	General.....	36
9.2	ST introduction (ASE_INT).....	36
9.2.1	Objectives.....	36
9.2.2	ASE_INT.1 ST introduction.....	36
9.3	Conformance claims (ASE_CCL).....	37
9.3.1	Objectives.....	37
9.3.2	ASE_CCL.1 Conformance claims.....	37
9.4	Security problem definition (ASE_SPD).....	39
9.4.1	Objectives.....	39
9.4.2	ASE_SPD.1 Security problem definition.....	39
9.5	Security objectives (ASE_OBJ).....	40
9.5.1	Objectives.....	40
9.5.2	Component levelling.....	40
9.5.3	ASE_OBJ.1 Security objectives for the operational environment.....	40
9.5.4	ASE_OBJ.2 Security objectives.....	41
9.6	Extended components definition (ASE_ECD).....	42

9.6.1	Objectives .....	42
9.6.2	ASE_ECD.1 Extended components definition .....	42
9.7	Security requirements (ASE_REQ).....	43
9.7.1	Objectives .....	43
9.7.2	Component levelling.....	43
9.7.3	ASE_REQ.1 Direct rationale security requirements.....	43
9.7.4	ASE_REQ.2 Derived security requirements.....	44
9.8	TOE summary specification (ASE_TSS) .....	45
9.8.1	Objectives .....	45
9.8.2	Component levelling.....	46
9.8.3	ASE_TSS.1 TOE summary specification.....	46
9.8.4	ASE_TSS.2 TOE summary specification with architectural design summary.....	46
9.9	Consistency of composite product Security Target (ASE_COMP).....	47
9.9.1	Objectives .....	47
9.9.2	Component levelling.....	47
9.9.3	Application notes .....	47
9.9.4	ASE_COMP.1 Consistency of Security Target (ST).....	48
<b>10</b>	<b>Class ADV: Development .....</b>	<b>49</b>
10.1	General.....	49
10.2	Security Architecture (ADV_ARC) .....	53
10.2.1	Objectives .....	53
10.2.2	Component levelling.....	53
10.2.3	Application notes .....	54
10.2.4	ADV_ARC.1 Security architecture description .....	54
10.3	Functional specification (ADV_FSP).....	55
10.3.1	Objectives .....	55
10.3.2	Component levelling.....	55
10.3.3	Application notes .....	56
10.3.4	ADV_FSP.1 Basic functional specification .....	58
10.3.5	ADV_FSP.2 Security-enforcing functional specification.....	59
10.3.6	ADV_FSP.3 Functional specification with complete summary.....	59
10.3.7	ADV_FSP.4 Complete functional specification.....	60
10.3.8	ADV_FSP.5 Complete semi-formal functional specification with additional error information .....	61
10.3.9	ADV_FSP.6 Complete semi-formal functional specification with additional formal specification.....	62
10.4	Implementation representation (ADV_IMP).....	63
10.4.1	Objectives .....	63
10.4.2	Component levelling.....	64
10.4.3	Application notes .....	64
10.4.4	ADV_IMP.1 Implementation representation of the TSF.....	65
10.4.5	ADV_IMP.2 Complete mapping of the implementation representation of the TSF .....	65
10.5	TSF internals (ADV_INT) .....	66
10.5.1	Objectives .....	66
10.5.2	Component levelling.....	66
10.5.3	Application notes .....	66
10.5.4	ADV_INT.1 Well-structured subset of TSF internals .....	67
10.5.5	ADV_INT.2 Well-structured internals.....	68
10.5.6	ADV_INT.3 Minimally complex internals.....	68
10.6	Security policy modelling (ADV_SPM).....	69
10.6.1	Objectives .....	69
10.6.2	Component levelling.....	70
10.6.3	Application notes .....	70
10.6.4	ADV_SPM.1 Formal TOE security policy model.....	70
10.7	TOE design (ADV_TDS) .....	72
10.7.1	Objectives .....	72
10.7.2	Component levelling.....	72

10.7.3	Application notes .....	72
10.7.4	ADV_TDS.1 Basic design .....	73
10.7.5	ADV_TDS.2 Architectural design .....	74
10.7.6	ADV_TDS.3 Basic modular design .....	75
10.7.7	ADV_TDS.4 Semiformal modular design .....	76
10.7.8	ADV_TDS.5 Complete semiformal modular design .....	78
10.7.9	ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation .....	79
10.8	Composite design compliance (ADV_COMP) .....	80
10.8.1	Objectives .....	80
10.8.2	Component levelling .....	80
10.8.3	Application notes .....	80
10.8.4	ADV_COMP.1 Design compliance with the base component-related user guidance, ETR for composite evaluation and report of the base component evaluation authority .....	81
<b>11</b>	<b>Class AGD: Guidance documents .....</b>	<b>82</b>
11.1	General .....	82
11.2	Operational user guidance (AGD_OPE) .....	82
11.2.1	Objectives .....	82
11.2.2	Component levelling .....	82
11.2.3	Application notes .....	82
11.2.4	AGD_OPE.1 Operational user guidance .....	83
11.3	Preparative procedures (AGD_PRE) .....	84
11.3.1	Objectives .....	84
11.3.2	Component levelling .....	84
11.3.3	Application notes .....	84
11.3.4	AGD_PRE.1 Preparative procedures .....	84
<b>12</b>	<b>Class ALC: Life-cycle support .....</b>	<b>85</b>
12.1	General .....	85
12.2	CM capabilities (ALC_CMC) .....	86
12.2.1	Objectives .....	86
12.2.2	Component levelling .....	87
12.2.3	Application notes .....	87
12.2.4	ALC_CMC.1 Labelling of the TOE .....	87
12.2.5	ALC_CMC.2 Use of the CM system .....	88
12.2.6	ALC_CMC.3 Authorization controls .....	89
12.2.7	ALC_CMC.4 Production support, acceptance procedures and automation .....	91
12.2.8	ALC_CMC.5 Advanced support .....	93
12.3	CM scope (ALC_CMS) .....	96
12.3.1	Objectives .....	96
12.3.2	Component levelling .....	96
12.3.3	Application notes .....	96
12.3.4	ALC_CMS.1 TOE CM coverage .....	96
12.3.5	ALC_CMS.2 Parts of the TOE CM coverage .....	97
12.3.6	ALC_CMS.3 Implementation representation CM coverage .....	98
12.3.7	ALC_CMS.4 Problem tracking CM coverage .....	99
12.3.8	ALC_CMS.5 Development tools CM coverage .....	99
12.4	Delivery (ALC_DEL) .....	100
12.4.1	Objectives .....	100
12.4.2	Component levelling .....	101
12.4.3	Application notes .....	101
12.4.4	ALC_DEL.1 Delivery procedures .....	101
12.5	Developer environment security (ALC_DVS) .....	102
12.5.1	Objectives .....	102
12.5.2	Component levelling .....	102
12.5.3	Application notes .....	102
12.5.4	ALC_DVS.1 Identification of security controls .....	102

12.5.5	ALC_DVS.2 Sufficiency of security controls	103
12.6	Flaw remediation (ALC_FLR)	103
12.6.1	Objectives	103
12.6.2	Component levelling	103
12.6.3	Application notes	103
12.6.4	ALC_FLR.1 Basic flaw remediation	104
12.6.5	ALC_FLR.2 Flaw reporting procedures	104
12.6.6	ALC_FLR.3 Systematic flaw remediation	106
12.7	Development Life-cycle definition (ALC_LCD)	107
12.7.1	Objectives	107
12.7.2	Component levelling	107
12.7.3	Application notes	108
12.7.4	ALC_LCD.1 Developer defined life-cycle processes	108
12.7.5	ALC_LCD.2 Measurable life-cycle model	109
12.8	TOE Development Artefacts (ALC_TDA)	110
12.8.1	Objectives	110
12.8.2	Component levelling	110
12.8.3	Application notes	110
12.8.4	ALC_TDA.1 Uniquely identifying implementation representation	111
12.8.5	ALC_TDA.2 Matching CMS scope of implementation representation	112
12.8.6	ALC_TDA.3 Regenerate TOE with well-defined development tools	114
12.9	Tools and techniques (ALC_TAT)	117
12.9.1	Objectives	117
12.9.2	Component levelling	117
12.9.3	Application notes	117
12.9.4	ALC_TAT.1 Well-defined development tools	118
12.9.5	ALC_TAT.2 Compliance with implementation standards	118
12.9.6	ALC_TAT.3 Compliance with implementation standards - all parts	119
12.10	Integration of composition parts and consistency check of delivery procedures (ALC_COMP)	120
12.10.1	Objectives	120
12.10.2	Component levelling	120
12.10.3	Application notes	120
12.10.4	ALC_COMP.1 Integration of the dependent component into the related base component and Consistency check for delivery and acceptance procedures	120
<b>13</b>	<b>Class ATE: Tests</b>	<b>121</b>
13.1	General	121
13.2	Coverage (ATE_COV)	122
13.2.1	Objectives	122
13.2.2	Component levelling	122
13.2.3	Application notes	122
13.2.4	ATE_COV.1 Evidence of coverage	122
13.2.5	ATE_COV.2 Analysis of coverage	123
13.2.6	ATE_COV.3 Rigorous analysis of coverage	123
13.3	Depth (ATE_DPT)	124
13.3.1	Objectives	124
13.3.2	Component levelling	124
13.3.3	Application notes	124
13.3.4	ATE_DPT.1 Testing: basic design	125
13.3.5	ATE_DPT.2 Testing: security enforcing modules	125
13.3.6	ATE_DPT.3 Testing: modular design	126
13.3.7	ATE_DPT.4 Testing: implementation representation	127
13.4	Functional tests (ATE_FUN)	128
13.4.1	Objectives	128
13.4.2	Component levelling	128
13.4.3	Application notes	128
13.4.4	ATE_FUN.1 Functional testing	128
13.4.5	ATE_FUN.2 Ordered functional testing	129