
**Information technology — Security
techniques — Evaluation criteria for IT
security —**

**Part 3:
Security assurance components**

*Technologies de l'information — Techniques de sécurité — Critères
d'évaluation pour la sécurité TI —*

Partie 3: Composants d'assurance de sécurité

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

1	Scope	1
2	Normative references	1
3	Terms and definitions, symbols and abbreviated terms	1
4	Overview	1
4.1	Organisation of this part of ISO/IEC 15408	1
5	Assurance paradigm	2
5.1	ISO/IEC 15408 philosophy	2
5.2	Assurance approach	2
5.2.1	Significance of vulnerabilities	2
5.2.2	Cause of vulnerabilities	3
5.2.3	ISO/IEC 15408 assurance	3
5.2.4	Assurance through evaluation	3
5.3	ISO/IEC 15408 evaluation assurance scale	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	8
6.2.1	EAL name	9
6.2.2	Objectives	9
6.2.3	Application notes	9
6.2.4	Assurance components	9
6.2.5	Relationship between assurances and assurance levels	10
6.3	CAP structure	10
6.3.1	CAP name	11
6.3.2	Objectives	11
6.3.3	Application notes	11
6.3.4	Assurance components	11
6.3.5	Relationship between assurances and assurance levels	12
7	Evaluation assurance levels	12
7.1	Evaluation assurance level (EAL) overview	13
7.2	Evaluation assurance level details	14
7.3	Evaluation assurance level 1 (EAL1) - functionally tested	14
7.3.1	Objectives	14
7.3.2	Assurance components	15
7.4	Evaluation assurance level 2 (EAL2) - structurally tested	15
7.4.1	Objectives	15
7.4.2	Assurance components	15
7.5	Evaluation assurance level 3 (EAL3) - methodically tested and checked	16
7.5.1	Objectives	16
7.5.2	Assurance components	16
7.6	Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed	17
7.6.1	Objectives	17
7.6.2	Assurance components	17
7.7	Evaluation assurance level 5 (EAL5) - semiformally designed and tested	18
7.7.1	Objectives	18
7.7.2	Assurance components	18
7.8	Evaluation assurance level 6 (EAL6) - semiformally verified design and tested	19

7.8.1	Objectives	19
7.8.2	Assurance components	19
7.9	Evaluation assurance level 7 (EAL7) - formally verified design and tested	20
7.9.1	Objectives	20
7.9.2	Assurance components	20
8	Composed assurance packages	21
8.1	Composed assurance package (CAP) overview	22
8.2	Composed assurance package details	23
8.3	Composition assurance level A (CAP-A) - Structurally composed	23
8.3.1	Objectives	23
8.3.2	Assurance components	23
8.4	Composition assurance level B (CAP-B) - Methodically composed	24
8.4.1	Objectives	24
8.4.2	Assurance components	24
8.5	Composition assurance level C (CAP-C) - Methodically composed, tested and reviewed	25
8.5.1	Objectives	25
8.5.2	Assurance components	25
9	Class APE: Protection Profile evaluation	26
9.1	PP introduction (APE_INT)	27
9.1.1	Objectives	27
9.1.2	APE_INT.1 PP introduction	27
9.2	Conformance claims (APE_CCL)	27
9.2.1	Objectives	27
9.2.2	APE_CCL.1 Conformance claims	27
9.3	Security problem definition (APE_SPD)	29
9.3.1	Objectives	29
9.3.2	APE_SPD.1 Security problem definition	29
9.4	Security objectives (APE_OBJ)	30
9.4.1	Objectives	30
9.4.2	Component levelling	30
9.4.3	APE_OBJ.1 Security objectives for the operational environment	30
9.4.4	APE_OBJ.2 Security objectives	30
9.5	Extended components definition (APE_ECD)	31
9.5.1	Objectives	31
9.5.2	APE_ECD.1 Extended components definition	32
9.6	Security requirements (APE_REQ)	32
9.6.1	Objectives	32
9.6.2	Component levelling	33
9.6.3	APE_REQ.1 Stated security requirements	33
9.6.4	APE_REQ.2 Derived security requirements	34
10	Class ASE: Security Target evaluation	35
10.1	ST introduction (ASE_INT)	35
10.1.1	Objectives	35
10.1.2	ASE_INT.1 ST introduction	35
10.2	Conformance claims (ASE_CCL)	36
10.2.1	Objectives	36
10.2.2	ASE_CCL.1 Conformance claims	37
10.3	Security problem definition (ASE_SPD)	38
10.3.1	Objectives	38
10.3.2	ASE_SPD.1 Security problem definition	38
10.4	Security objectives (ASE_OBJ)	39
10.4.1	Objectives	39
10.4.2	Component levelling	39
10.4.3	ASE_OBJ.1 Security objectives for the operational environment	39
10.4.4	ASE_OBJ.2 Security objectives	39
10.5	Extended components definition (ASE_ECD)	40
10.5.1	Objectives	40
10.5.2	ASE_ECD.1 Extended components definition	40

10.6	Security requirements (ASE_REQ).....	41
10.6.1	Objectives	41
10.6.2	Component levelling	42
10.6.3	ASE_REQ.1 Stated security requirements.....	42
10.6.4	ASE_REQ.2 Derived security requirements	42
10.7	TOE summary specification (ASE_TSS)	44
10.7.1	Objectives	44
10.7.2	Component levelling	44
10.7.3	ASE_TSS.1 TOE summary specification.....	44
10.7.4	ASE_TSS.2 TOE summary specification with architectural design summary	44
11	Class ADV: Development.....	45
11.1	Security Architecture (ADV_ARC)	50
11.1.1	Objectives	50
11.1.2	Component levelling	50
11.1.3	Application notes	50
11.1.4	ADV_ARC.1 Security architecture description.....	51
11.2	Functional specification (ADV_FSP)	52
11.2.1	Objectives	52
11.2.2	Component levelling	52
11.2.3	Application notes	52
11.2.4	ADV_FSP.1 Basic functional specification	54
11.2.5	ADV_FSP.2 Security-enforcing functional specification.....	55
11.2.6	ADV_FSP.3 Functional specification with complete summary	56
11.2.7	ADV_FSP.4 Complete functional specification	57
11.2.8	ADV_FSP.5 Complete semi-formal functional specification with additional error information	58
11.2.9	ADV_FSP.6 Complete semi-formal functional specification with additional formal specification.....	59
11.3	Implementation representation (ADV_IMP)	61
11.3.1	Objectives	61
11.3.2	Component levelling	61
11.3.3	Application notes	61
11.3.4	ADV_IMP.1 Implementation representation of the TSF	62
11.3.5	ADV_IMP.2 Complete mapping of the implementation representation of the TSF.....	62
11.4	TSF internals (ADV_INT).....	63
11.4.1	Objectives	63
11.4.2	Component levelling	63
11.4.3	Application notes	63
11.4.4	ADV_INT.1 Well-structured subset of TSF internals.....	64
11.4.5	ADV_INT.2 Well-structured internals.....	65
11.4.6	ADV_INT.3 Minimally complex internals	66
11.5	Security policy modelling (ADV_SPM)	67
11.5.1	Objectives	67
11.5.2	Component levelling	67
11.5.3	Application notes	67
11.5.4	ADV_SPM.1 Formal TOE security policy model.....	68
11.6	TOE design (ADV_TDS)	69
11.6.1	Objectives	69
11.6.2	Component levelling	69
11.6.3	Application notes	69
11.6.4	ADV_TDS.1 Basic design.....	70
11.6.5	ADV_TDS.2 Architectural design	71
11.6.6	ADV_TDS.3 Basic modular design	72
11.6.7	ADV_TDS.4 Semiformal modular design	74
11.6.8	ADV_TDS.5 Complete semiformal modular design	75
11.6.9	ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation	76
12	Class AGD: Guidance documents	78
12.1	Operational user guidance (AGD_OPE).....	78

12.1.1	Objectives.....	78
12.1.2	Component levelling	78
12.1.3	Application notes.....	79
12.1.4	AGD_OPE.1 Operational user guidance.....	79
12.2	Preparative procedures (AGD_PRE).....	80
12.2.1	Objectives.....	80
12.2.2	Component levelling	80
12.2.3	Application notes.....	80
12.2.4	AGD_PRE.1 Preparative procedures	81
13	Class ALC: Life-cycle support.....	81
13.1	CM capabilities (ALC_CMC).....	82
13.1.1	Objectives.....	82
13.1.2	Component levelling	82
13.1.3	Application notes.....	83
13.1.4	ALC_CMC.1 Labelling of the TOE	83
13.1.5	ALC_CMC.2 Use of a CM system	84
13.1.6	ALC_CMC.3 Authorisation controls.....	85
13.1.7	ALC_CMC.4 Production support, acceptance procedures and automation	86
13.1.8	ALC_CMC.5 Advanced support.....	88
13.2	CM scope (ALC_CMS)	90
13.2.1	Objectives.....	90
13.2.2	Component levelling	91
13.2.3	Application notes.....	91
13.2.4	ALC_CMS.1 TOE CM coverage.....	91
13.2.5	ALC_CMS.2 Parts of the TOE CM coverage.....	91
13.2.6	ALC_CMS.3 Implementation representation CM coverage	92
13.2.7	ALC_CMS.4 Problem tracking CM coverage	93
13.2.8	ALC_CMS.5 Development tools CM coverage.....	94
13.3	Delivery (ALC_DEL).....	95
13.3.1	Objectives.....	95
13.3.2	Component levelling	95
13.3.3	Application notes.....	95
13.3.4	ALC_DEL.1 Delivery procedures.....	96
13.4	Development security (ALC_DVS)	96
13.4.1	Objectives.....	96
13.4.2	Component levelling	96
13.4.3	Application notes.....	96
13.4.4	ALC_DVS.1 Identification of security measures	97
13.4.5	ALC_DVS.2 Sufficiency of security measures.....	97
13.5	Flaw remediation (ALC_FLR).....	98
13.5.1	Objectives.....	98
13.5.2	Component levelling	98
13.5.3	Application notes.....	98
13.5.4	ALC_FLR.1 Basic flaw remediation	98
13.5.5	ALC_FLR.2 Flaw reporting procedures	99
13.5.6	ALC_FLR.3 Systematic flaw remediation	100
13.6	Life-cycle definition (ALC_LCD).....	102
13.6.1	Objectives.....	102
13.6.2	Component levelling	102
13.6.3	Application notes.....	102
13.6.4	ALC_LCD.1 Developer defined life-cycle model.....	103
13.6.5	ALC_LCD.2 Measurable life-cycle model	104
13.7	Tools and techniques (ALC_TAT).....	104
13.7.1	Objectives.....	104
13.7.2	Component levelling	105
13.7.3	Application notes.....	105
13.7.4	ALC_TAT.1 Well-defined development tools	105
13.7.5	ALC_TAT.2 Compliance with implementation standards.....	106
13.7.6	ALC_TAT.3 Compliance with implementation standards - all parts.....	106

14	Class ATE: Tests	107
14.1	Coverage (ATE_COV)	108
14.1.1	Objectives	108
14.1.2	Component levelling	108
14.1.3	Application notes	108
14.1.4	ATE_COV.1 Evidence of coverage	108
14.1.5	ATE_COV.2 Analysis of coverage	109
14.1.6	ATE_COV.3 Rigorous analysis of coverage	109
14.2	Depth (ATE_DPT)	110
14.2.1	Objectives	110
14.2.2	Component levelling	111
14.2.3	Application notes	111
14.2.4	ATE_DPT.1 Testing: basic design	111
14.2.5	ATE_DPT.2 Testing: security enforcing modules	112
14.2.6	ATE_DPT.3 Testing: modular design	112
14.2.7	ATE_DPT.4 Testing: implementation representation	113
14.3	Functional tests (ATE_FUN)	114
14.3.1	Objectives	114
14.3.2	Component levelling	114
14.3.3	Application notes	114
14.3.4	ATE_FUN.1 Functional testing	115
14.3.5	ATE_FUN.2 Ordered functional testing	115
14.4	Independent testing (ATE_IND)	116
14.4.1	Objectives	116
14.4.2	Component levelling	116
14.4.3	Application notes	117
14.4.4	ATE_IND.1 Independent testing - conformance	117
14.4.5	ATE_IND.2 Independent testing - sample	118
14.4.6	ATE_IND.3 Independent testing - complete	119
15	Class AVA: Vulnerability assessment	120
15.1	Application notes	120
15.2	Vulnerability analysis (AVA_VAN)	121
15.2.1	Objectives	121
15.2.2	Component levelling	121
15.2.3	AVA_VAN.1 Vulnerability survey	121
15.2.4	AVA_VAN.2 Vulnerability analysis	122
15.2.5	AVA_VAN.3 Focused vulnerability analysis	123
15.2.6	AVA_VAN.4 Methodical vulnerability analysis	124
15.2.7	AVA_VAN.5 Advanced methodical vulnerability analysis	125
16	Class ACO: Composition	126
16.1	Composition rationale (ACO_COR)	128
16.1.1	Objectives	128
16.1.2	Component levelling	128
16.1.3	ACO_COR.1 Composition rationale	128
16.2	Development evidence (ACO_DEV)	129
16.2.1	Objectives	129
16.2.2	Component levelling	129
16.2.3	Application notes	129
16.2.4	ACO_DEV.1 Functional Description	130
16.2.5	ACO_DEV.2 Basic evidence of design	130
16.2.6	ACO_DEV.3 Detailed evidence of design	131
16.3	Reliance of dependent component (ACO_REL)	132
16.3.1	Objectives	132
16.3.2	Component levelling	132
16.3.3	Application notes	133
16.3.4	ACO_REL.1 Basic reliance information	133
16.3.5	ACO_REL.2 Reliance information	133
16.4	Composed TOE testing (ACO_CTT)	134
16.4.1	Objectives	134

16.4.2	Component levelling	134
16.4.3	Application notes.....	134
16.4.4	ACO_CTT.1 Interface testing	135
16.4.5	ACO_CTT.2 Rigorous interface testing	136
16.5	Composition vulnerability analysis (ACO_VUL).....	137
16.5.1	Objectives.....	137
16.5.2	Component levelling	137
16.5.3	Application notes.....	138
16.5.4	ACO_VUL.1 Composition vulnerability review	138
16.5.5	ACO_VUL.2 Composition vulnerability analysis	139
16.5.6	ACO_VUL.3 Enhanced-Basic Composition vulnerability analysis.....	139
Annex A	(informative) Development (ADV).....	141
A.1	ADV_ARC: Supplementary material on security architectures	141
A.1.1	Security architecture properties	141
A.1.2	Security architecture descriptions.....	142
A.2	ADV_FSP: Supplementary material on TSFIs.....	144
A.2.1	Determining the TSFI.....	144
A.2.2	Example: A complex DBMS.....	146
A.2.3	Example Functional Specification	147
A.3	ADV_INT: Supplementary material on TSF internals	149
A.3.1	Structure of procedural software.....	149
A.3.2	Complexity of procedural software.....	151
A.4	ADV_TDS: Subsystems and Modules.....	151
A.4.1	Subsystems.....	152
A.4.2	Modules	152
A.4.3	Levelling Approach.....	154
A.5	Supplementary material on formal methods	156
Annex B	(informative) Composition (ACO).....	158
B.1	Necessity for composed TOE evaluations.....	158
B.2	Performing Security Target evaluation for a composed TOE	159
B.3	Interactions between composed IT entities	160
Annex C	(informative) Cross reference of assurance component dependencies.....	165
Annex D	(informative) Cross reference of PPs and assurance components.....	169
Annex E	(informative) Cross reference of EALs and assurance components	170
Annex F	(informative) Cross reference of CAPs and assurance components	171

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15408-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. The identical text of ISO/IEC 15408 is published by the Common Criteria Project Sponsoring Organisations as Common Criteria for Information Technology Security Evaluation. The common XML source for both publications can be found at <http://www.oc.ccn.cni.es/xml>

This third edition cancels and replaces the second edition (ISO/IEC 15408-3:2005), which has been technically revised.

ISO/IEC 15408 consists of the following parts, under the general title *Information technology — Security techniques — Evaluation criteria for IT security*:

- *Part 1: Introduction and general model*
- *Part 2: Security functional components*
- *Part 3: Security assurance components*

Legal Notice

The governmental organizations listed below contributed to the development of this version of the Common Criteria for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Criteria for Information Technology Security Evaluations, version 3.1 Parts 1 through 3 (called CC 3.1), they hereby grant non-exclusive license to ISO/IEC to use CC 3.1 in the continued development/maintenance of the ISO/IEC 15408 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CC 3.1 as they see fit.

Australia/New Zealand:	The Defence Signals Directorate and the Government Communications Security Bureau respectively;
Canada:	Communications Security Establishment;
France:	Direction Centrale de la Sécurité des Systèmes d'Information;
Germany:	Bundesamt für Sicherheit in der Informationstechnik;
Japan:	Information Technology Promotion Agency;

ISO/IEC 15408-3:2008(E)

Netherlands:	Netherlands National Communications Security Agency;
Spain:	Ministerio de Administraciones Públicas and Centro Criptológico Nacional;
United Kingdom:	Communications-Electronic Security Group;
United States:	The National Security Agency and the National Institute of Standards and Technology.

Introduction

Security assurance components, as defined in this part of ISO/IEC 15408, are the basis for the security assurance requirements expressed in a Protection Profile (PP) or a Security Target (ST).

These requirements establish a standard way of expressing the assurance requirements for TOEs. This part of ISO/IEC 15408 catalogues the set of assurance components, families and classes. This part of ISO/IEC 15408 also defines evaluation criteria for PPs and STs and presents evaluation assurance levels that define the predefined ISO/IEC 15408 scale for rating assurance for TOEs, which is called the Evaluation Assurance Levels (EALs).

The audience for this part of ISO/IEC 15408 includes consumers, developers, and evaluators of secure IT products. ISO/IEC 15408-1 provides additional information on the target audience of ISO/IEC 15408, and on the use of IEC 15408 by the groups that comprise the target audience. These groups may use this part of ISO/IEC 15408 as follows:

- a) Consumers, who use this part of ISO/IEC 15408 when selecting components to express assurance requirements to satisfy the security objectives expressed in a PP or ST, determining required levels of security assurance of the TOE.
- b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, reference this part of ISO/IEC 15408 when interpreting statements of assurance requirements and determining assurance approaches of TOEs.
- c) Evaluators, who use the assurance requirements defined in this part of ISO/IEC 15408 as a mandatory statement of evaluation criteria when determining the assurance of TOEs and when evaluating PPs and STs.

Information technology — Security techniques — Evaluation criteria for IT security —

Part 3: Security assurance components

1 Scope

This part of ISO/IEC 15408 defines the assurance requirements of ISO/IEC 15408. It includes the evaluation assurance levels (EALs) that define a scale for measuring assurance for component TOEs, the composed assurance packages (CAPs) that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of PPs and STs.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*