
**Information technology — Security
techniques — Methodology for IT security
evaluation**

*Technologies de l'information — Techniques de sécurité —
Méthodologie pour l'évaluation de sécurité TI*

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.

This document is a preview generated by EVS



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	1
4	Symbols and abbreviated terms	3
5	Overview	3
5.1	Organisation of this International Standard	3
6	Document Conventions	3
6.1	Terminology	3
6.2	Verb usage	3
6.3	General evaluation guidance	4
6.4	Relationship between ISO/IEC 15408 and ISO/IEC 18045 structures	4
7	Evaluation process and related tasks	4
7.1	Introduction	4
7.2	Evaluation process overview	5
7.2.1	Objectives	5
7.2.2	Responsibilities of the roles	5
7.2.3	Relationship of roles	5
7.2.4	General evaluation model	6
7.2.5	Evaluator verdicts	6
7.3	Evaluation input task	8
7.3.1	Objectives	8
7.3.2	Application notes	8
7.3.3	Management of evaluation evidence sub-task	8
7.4	Evaluation sub-activities	9
7.5	Evaluation output task	9
7.5.1	Objectives	9
7.5.2	Management of evaluation outputs	9
7.5.3	Application notes	10
7.5.4	Write OR sub-task	10
7.5.5	Write ETR sub-task	10
8	Class APE: Protection Profile evaluation	15
8.1	Introduction	15
8.2	Application notes	15
8.2.1	Re-using the evaluation results of certified PPs	15
8.3	PP introduction (APE_INT)	16
8.3.1	Evaluation of sub-activity (APE_INT.1)	16
8.4	Conformance claims (APE_CCL)	17
8.4.1	Evaluation of sub-activity (APE_CCL.1)	17
8.5	Security problem definition (APE_SPD)	21
8.5.1	Evaluation of sub-activity (APE_SPD.1)	21
8.6	Security objectives (APE_OBJ)	23
8.6.1	Evaluation of sub-activity (APE_OBJ.1)	23
8.6.2	Evaluation of sub-activity (APE_OBJ.2)	23
8.7	Extended components definition (APE_ECD)	25
8.7.1	Evaluation of sub-activity (APE_ECD.1)	25
8.8	Security requirements (APE_REQ)	29
8.8.1	Evaluation of sub-activity (APE_REQ.1)	29
8.8.2	Evaluation of sub-activity (APE_REQ.2)	32
9	Class ASE: Security Target evaluation	36
9.1	Introduction	36

9.2	Application notes.....	37
9.2.1	Re-using the evaluation results of certified PPs	37
9.3	ST introduction (ASE_INT).....	37
9.3.1	Evaluation of sub-activity (ASE_INT.1)	37
9.4	Conformance claims (ASE_CCL)	40
9.4.1	Evaluation of sub-activity (ASE_CCL.1).....	40
9.5	Security problem definition (ASE_SPD).....	45
9.5.1	Evaluation of sub-activity (ASE_SPD.1).....	45
9.6	Security objectives (ASE_OBJ).....	47
9.6.1	Evaluation of sub-activity (ASE_OBJ.1).....	47
9.6.2	Evaluation of sub-activity (ASE_OBJ.2).....	47
9.7	Extended components definition (ASE_ECD)	49
9.7.1	Evaluation of sub-activity (ASE_ECD.1).....	49
9.8	Security requirements (ASE_REQ)	53
9.8.1	Evaluation of sub-activity (ASE_REQ.1)	53
9.8.2	Evaluation of sub-activity (ASE_REQ.2)	56
9.9	TOE summary specification (ASE_TSS)	60
9.9.1	Evaluation of sub-activity (ASE_TSS.1)	60
9.9.2	Evaluation of sub-activity (ASE_TSS.2)	61
10	Class ADV: Development.....	62
10.1	Introduction	62
10.2	Application notes.....	63
10.3	Security Architecture (ADV_ARC).....	63
10.3.1	Evaluation of sub-activity (ADV_ARC.1).....	63
10.4	Functional specification (ADV_FSP).....	67
10.4.1	Evaluation of sub-activity (ADV_FSP.1).....	67
10.4.2	Evaluation of sub-activity (ADV_FSP.2).....	70
10.4.3	Evaluation of sub-activity (ADV_FSP.3).....	75
10.4.4	Evaluation of sub-activity (ADV_FSP.4).....	80
10.4.5	Evaluation of sub-activity (ADV_FSP.5).....	85
10.4.6	Evaluation of sub-activity (ADV_FSP.6).....	90
10.5	Implementation representation (ADV_IMP).....	90
10.5.1	Evaluation of sub-activity (ADV_IMP.1).....	90
10.5.2	Evaluation of sub-activity (ADV_IMP.2).....	92
10.6	TSF internals (ADV_INT)	93
10.6.1	Evaluation of sub-activity (ADV_INT.1)	93
10.6.2	Evaluation of sub-activity (ADV_INT.2)	95
10.6.3	Evaluation of sub-activity (ADV_INT.3)	97
10.7	Security policy modelling (ADV_SPM)	97
10.7.1	Evaluation of sub-activity (ADV_SPM.1)	97
10.8	TOE design (ADV_TDS).....	97
10.8.1	Evaluation of sub-activity (ADV_TDS.1).....	97
10.8.2	Evaluation of sub-activity (ADV_TDS.2).....	100
10.8.3	Evaluation of sub-activity (ADV_TDS.3).....	105
10.8.4	Evaluation of sub-activity (ADV_TDS.4).....	113
10.8.5	Evaluation of sub-activity (ADV_TDS.5).....	122
10.8.6	Evaluation of sub-activity (ADV_TDS.6).....	122
11	Class AGD: Guidance documents	122
11.1	Introduction	122
11.2	Application notes.....	122
11.3	Operational user guidance (AGD_OPE)	122
11.3.1	Evaluation of sub-activity (AGD_OPE.1)	122
11.4	Preparative procedures (AGD_PRE).....	125
11.4.1	Evaluation of sub-activity (AGD_PRE.1)	125
12	Class ALC: Life-cycle support.....	127
12.1	Introduction	127
12.2	CM capabilities (ALC_CMC).....	127
12.2.1	Evaluation of sub-activity (ALC_CMC.1)	127

12.2.2	Evaluation of sub-activity (ALC_CMC.2)	128
12.2.3	Evaluation of sub-activity (ALC_CMC.3)	130
12.2.4	Evaluation of sub-activity (ALC_CMC.4)	133
12.2.5	Evaluation of sub-activity (ALC_CMC.5)	139
12.3	CM scope (ALC_CMS)	145
12.3.1	Evaluation of sub-activity (ALC_CMS.1)	145
12.3.2	Evaluation of sub-activity (ALC_CMS.2)	146
12.3.3	Evaluation of sub-activity (ALC_CMS.3)	147
12.3.4	Evaluation of sub-activity (ALC_CMS.4)	148
12.3.5	Evaluation of sub-activity (ALC_CMS.5)	149
12.4	Delivery (ALC_DEL)	150
12.4.1	Evaluation of sub-activity (ALC_DEL.1)	150
12.5	Development security (ALC_DVS)	152
12.5.1	Evaluation of sub-activity (ALC_DVS.1)	152
12.5.2	Evaluation of sub-activity (ALC_DVS.2)	154
12.6	Flaw remediation (ALC_FLR)	157
12.6.1	Evaluation of sub-activity (ALC_FLR.1)	157
12.6.2	Evaluation of sub-activity (ALC_FLR.2)	159
12.6.3	Evaluation of sub-activity (ALC_FLR.3)	162
12.7	Life-cycle definition (ALC_LCD)	167
12.7.1	Evaluation of sub-activity (ALC_LCD.1)	167
12.7.2	Evaluation of sub-activity (ALC_LCD.2)	168
12.8	Tools and techniques (ALC_TAT)	170
12.8.1	Evaluation of sub-activity (ALC_TAT.1)	170
12.8.2	Evaluation of sub-activity (ALC_TAT.2)	171
12.8.3	Evaluation of sub-activity (ALC_TAT.3)	174
13	Class ATE: Tests	176
13.1	Introduction	176
13.2	Application notes	176
13.2.1	Understanding the expected behaviour of the TOE	177
13.2.2	Testing vs. alternate approaches to verify the expected behaviour of functionality	177
13.2.3	Verifying the adequacy of tests	177
13.3	Coverage (ATE_COV)	178
13.3.1	Evaluation of sub-activity (ATE_COV.1)	178
13.3.2	Evaluation of sub-activity (ATE_COV.2)	179
13.3.3	Evaluation of sub-activity (ATE_COV.3)	180
13.4	Depth (ATE_DPT)	180
13.4.1	Evaluation of sub-activity (ATE_DPT.1)	180
13.4.2	Evaluation of sub-activity (ATE_DPT.2)	182
13.4.3	Evaluation of sub-activity (ATE_DPT.3)	184
13.4.4	Evaluation of sub-activity (ATE_DPT.4)	186
13.5	Functional tests (ATE_FUN)	187
13.5.1	Evaluation of sub-activity (ATE_FUN.1)	187
13.5.2	Evaluation of sub-activity (ATE_FUN.2)	189
13.6	Independent testing (ATE_IND)	190
13.6.1	Evaluation of sub-activity (ATE_IND.1)	190
13.6.2	Evaluation of sub-activity (ATE_IND.2)	193
13.6.3	Evaluation of sub-activity (ATE_IND.3)	198
14	Class AVA: Vulnerability assessment	198
14.1	Introduction	198
14.2	Vulnerability analysis (AVA_VAN)	198
14.2.1	Evaluation of sub-activity (AVA_VAN.1)	198
14.2.2	Evaluation of sub-activity (AVA_VAN.2)	203
14.2.3	Evaluation of sub-activity (AVA_VAN.3)	209
14.2.4	Evaluation of sub-activity (AVA_VAN.4)	217
14.2.5	Evaluation of sub-activity (AVA_VAN.5)	224
15	Class ACO: Composition	224
15.1	Introduction	224

15.2	Application notes	224
15.3	Composition rationale (ACO_COR)	225
15.3.1	Evaluation of sub-activity (ACO_COR.1)	225
15.4	Development evidence (ACO_DEV)	231
15.4.1	Evaluation of sub-activity (ACO_DEV.1)	231
15.4.2	Evaluation of sub-activity (ACO_DEV.2)	232
15.4.3	Evaluation of sub-activity (ACO_DEV.3)	234
15.5	Reliance of dependent component (ACO_REL)	236
15.5.1	Evaluation of sub-activity (ACO_REL.1)	236
15.5.2	Evaluation of sub-activity (ACO_REL.2)	238
15.6	Composed TOE testing (ACO_CTT)	241
15.6.1	Evaluation of sub-activity (ACO_CTT.1)	241
15.6.2	Evaluation of sub-activity (ACO_CTT.2)	243
15.7	Composition vulnerability analysis (ACO_VUL)	246
15.7.1	Evaluation of sub-activity (ACO_VUL.1)	246
15.7.2	Evaluation of sub-activity (ACO_VUL.2)	249
15.7.3	Evaluation of sub-activity (ACO_VUL.3)	252
Annex A	(informative) General evaluation guidance	257
A.1	Objectives	257
A.2	Sampling	257
A.3	Dependencies	259
A.3.1	Dependencies between activities	259
A.3.2	Dependencies between sub-activities	259
A.3.3	Dependencies between actions	259
A.4	Site Visits	259
A.4.1	Introduction	259
A.4.2	General Approach	260
A.4.3	Orientation Guide for the Preparation of the Check List	261
A.4.4	Example of a checklist	262
A.5	Scheme Responsibilities	264
Annex B	(informative) Vulnerability Assessment (AVA)	266
B.1	What is Vulnerability Analysis	266
B.2	Evaluator construction of a Vulnerability Analysis	266
B.2.1	Generic vulnerability guidance	267
B.2.2	Identification of Potential Vulnerabilities	274
B.3	When attack potential is used	276
B.3.1	Developer	276
B.3.2	Evaluator	277
B.4	Calculating attack potential	278
B.4.1	Application of attack potential	278
B.4.2	Characterising attack potential	278
B.5	Example calculation for direct attack	284

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 18045 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*. The identical text of ISO/IEC 18045 is published by the Common Criteria Project Sponsoring Organisations as *Common Methodology for Information Technology Security Evaluation*. The common XML source for both publications can be found at <http://www.oc.ccn.cni.es/xml>.

This second edition cancels and replaces the first edition (ISO/IEC 18045:2005), which has been technically revised.

Legal Notice

The governmental organizations listed below contributed to the development of this version of the Common Methodology for Information Technology Security Evaluations. As the joint holders of the copyright in the Common Methodology for Information Technology Security Evaluations, version 3.1 (called CEM 3.1), they hereby grant non-exclusive license to ISO/IEC to use CEM 3.1 in the continued development/maintenance of the ISO/IEC 18045 international standard. However, these governmental organizations retain the right to use, copy, distribute, translate or modify CEM 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;
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

The target audience for this International Standard is primarily evaluators applying ISO/IEC 15408 and certifiers confirming evaluator actions; evaluation sponsors, developers, PP/ST authors and other parties interested in IT security are a secondary audience.

This International Standard recognises that not all questions concerning IT security evaluation will be answered herein and that further interpretations will be needed. Individual schemes will determine how to handle such interpretations, although these can be subject to mutual recognition agreements. A list of methodology-related activities that can be handled by individual schemes can be found in Annex A.

This document is a preview generated by EVS

Information technology — Security techniques — Methodology for IT security evaluation

1 Scope

This International Standard is a companion document to the evaluation criteria for IT security defined in ISO/IEC 15408. It defines the minimum actions to be performed by an evaluator in order to conduct an ISO/IEC 15408 evaluation, using the criteria and evaluation evidence defined in ISO/IEC 15408.

This International Standard does not define evaluator actions for certain high assurance ISO/IEC 15408 components, where there is as yet no generally agreed guidance.

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 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

NOTE Terms which are presented in bold-faced type are themselves defined in this clause.

3.1

action

evaluator action element of ISO/IEC 15408-3

NOTE These actions are either explicitly stated as evaluator actions or implicitly derived from developer actions (implied evaluator actions) within ISO/IEC 15408-3 assurance components.

3.2

activity

application of an assurance class of ISO/IEC 15408-3

3.3

check

generate a **verdict** by a simple comparison

NOTE Evaluator expertise is not required. The statement that uses this verb describes what is mapped.

3.4

evaluation deliverable

any resource required from the sponsor or developer by the evaluator or evaluation authority to perform one or more evaluation or evaluation oversight activities

3.5

evaluation evidence

tangible **evaluation deliverable**